Privacy by Design in Law, Policy and Practice

David Goodis
Director of Legal Services and General Counsel

Stephen McCammon
Legal Counsel

Office of the Information and Privacy Commissioner / Ontario

IAPP
May 10, 2012
Presentation Outline

1. What is \textit{PbD} and why do we need to change the privacy paradigm?

2. \textit{Privacy by Design} in Law, Policy and Practice
   - Regulatory Approaches
   - Organizational Approaches
   - Enforcement & Remedial Approaches
Why We Need *Privacy by Design*

Complaint driven compliance unsustainable as sole model for ensuring future of privacy

Most privacy breaches remain undetected and unknown – we only see the tip of the iceberg
Beware of “Surveillance by Design:”
Stand Up for Freedom and Privacy
January 27, 2012
## Mapping FIPPs → Meta-FIPPs

<table>
<thead>
<tr>
<th>Safeguards</th>
<th>Data Minimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose Specification</td>
<td>Consent</td>
</tr>
<tr>
<td>Collection Limitation</td>
<td>Accuracy</td>
</tr>
<tr>
<td>Use, Retention and Disclosure Limitation</td>
<td>Access</td>
</tr>
<tr>
<td></td>
<td>Redress</td>
</tr>
<tr>
<td></td>
<td>Accountability (beyond data subject)</td>
</tr>
</tbody>
</table>

- Safeguards
- Purpose Specification
  - Collection Limitation
  - Use, Retention and Disclosure Limitation
- Consent
- Accuracy
- Access
- Redress
- Accountability
  - Openness
  - Compliance
## Mapping Meta-FIPPs → PbD

<table>
<thead>
<tr>
<th>Safeguards</th>
<th>End to End Lifecycle Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Minimization</td>
<td>Privacy as the Default (Setting)</td>
</tr>
<tr>
<td>User Participation</td>
<td>Respect for User Privacy</td>
</tr>
<tr>
<td>Accountability</td>
<td>Openness &amp; Transparency</td>
</tr>
<tr>
<td>Leadership &amp; Goal-Setting</td>
<td>Proactive Not Reaction; Preventative Not Remedial</td>
</tr>
<tr>
<td>Verifiable Methods</td>
<td>Privacy Embedded into Design</td>
</tr>
<tr>
<td>Quantitative Results</td>
<td>Full Functionality – Positive-Sum, not Zero-Sum</td>
</tr>
</tbody>
</table>
Privacy by Design: The Next Generation of Privacy Protection

- Incorporating PbD into law, policy and practice means taking a proactive approach to privacy that is both more robust, and yet more flexible than traditional ones.

- Calls for a privacy informed approach to all relevant process and system decision making and design.

- PbD is necessarily flexible – no single way to roll out.
The Three *PbD* Application Zones

- Information Technology
- Accountable Business Practices
- Physical Design & Networked Infrastructure
Privacy by Design:
Multiple benefits of embedding privacy

• Improved **customer confidence**, trust and loyalty

• **Efficiencies and risk reduction** flowing from handling only personal information that is necessary to business processes

• **Cost savings** as a result of building privacy in up front rather than having to bolt it on, after the fact

• Reduction of exposure to liability associated with privacy breaches

• **Gaining a competitive advantage** in the market
Privacy by Design in Law, Policy and Practice
Privacy by Design  adopted as an International Standard (October 29, 2010 –Jerusalem)

The 32nd gathering of International of Data Protection and Privacy Commissioners resolved to:

1. Recognize Privacy by Design as an essential component of fundamental privacy protection
2. Encourage the adoption of the Foundational Principles of Privacy by Design as guidance to establishing privacy as an organization’s default mode of operation
3. Invite Data Protection and Privacy Commissioners to:
   a. promote Privacy by Design as widely as possible through distribution of materials, education and personal advocacy
   b. foster the incorporation of the Privacy by Design Foundational Principles in the formulation of privacy policy and legislation within their respective jurisdictions
PbD and Omnibus Privacy Legislation

Ideally, omnibus legislation should provide for PbD. Models:

• Jan. 2012 Draft EU Privacy Regulation allows the EU Commission to specify the “criteria and conditions” for “privacy by design and data protection by default” solutions for “specific sectors and in specific data processing situations” (article 30)

• May 2011, Kerry and McCain propose Commercial Privacy Bill of Rights (SB 799) - would require businesses to implement a “comprehensive [“Privacy by Design “] information privacy program” throughout their product life cycles (s. 103)

• PIPEDA does not mention PbD. However, in her 2010 Online Cloud Computing Report, the OPC said that it “will work with Industry Canada to consider how best to integrate privacy by design principles and PIAs into private sector practices”
Smart Grid legislation provides functional specifications that electricity distributors must adhere to in order to achieve smart meter policy goals.

To build consumer confidence and trust and secure privacy, Commissioner Cavoukian says “integrate PbD into the Grid”

Ontario Minister of Energy’s 2010 Smart Grid Directive requires that, in performing its functions, the Ontario Energy Board be guided by policy objectives including:

“Privacy: Respect and protect the privacy of customers. Integrate privacy requirements into smart grid planning and design from an early stage, including the completion of privacy impact assessments.”
Smart Grid Sectoral Laws (con’t)

California Public Utility Commission decisions adopt rules to protect the privacy and security of customer electricity usage data (Rulemaking 08-12-009, Decision 11-07-056, July 28, 2011)

• Based on Fair Information Practice Principles
• Rules apply to utilities, utility third-party contractors and third parties accessing customer information directly from the utility
• Customer consent not required for primary purposes such as utility operations, energy efficiency, demand response or energy management programs – all other purposes are considered secondary purposes and require positive customer authorization
• “…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” (p. 73)
U.S. regulator urges integration of *PbD* into business practices

March 2012 - final FTC privacy framework and implementation recommendations:

“**PRIVACY BY DESIGN**

**Baseline Principle:** Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services”

“…Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.”

“…Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.”

www.privacybydesign.ca
Organizational Approaches to PbD

• Adoption of PbD by an organization or company will build business and competitive advantages.

• PbD should be implemented across an entire organization, including IT systems, business practices and product design.

• PbD encourages executives to understand customer and stakeholder expectations of privacy within their own context and industry.
IBM recognizes that the implementation of *PbD* creates “value beyond its original goals”

IBM’s approach to implementing *PbD* throughout global enterprise:

- Focus the privacy team on counseling and supporting the business rather than laborious administration
- Start small, learn, then expand
- Develop easy to use, dynamic tools designed to provide business intelligence and direction
Applying PbD Best Practices to SDG&E’s Dynamic Pricing System
March 2012 IPC / San Diego Gas & Electric Paper

• SDG&E’s smart meter privacy governance framework includes:
  • A customer privacy program grounded in responsibility for customer data and respect for customer;
  • Enterprise information risk management – a standard framework for continually managing, measuring and improving information risk;
  • The executive management team role of the Chief Privacy Officer;
  • Engineering privacy into products;
  • Role based employee rights and responsibilities; and
  • Privacy and security features embedded into vendor/service provider contracts.
Embedding Privacy into the Design of Electronic Health Records
March 2, 2012 IPC / Canada Health Infoway Paper

• A “Big Privacy” response to “Big Data”
• Leverage information technology to ensure principled and effective data handling and governance.
• Ensure that the default condition for all secondary uses and disclosures of personal health information is de-identification.
Do Not Track - Digital Advertising
Industry wrestles with *PbD*

- February 2012 - In response to escalating privacy concerns and mounting calls for privacy legislation, Google, Microsoft, Yahoo, AOL and hundreds of other companies in the Digital Advertising Alliance promised to work with the major Web browsers to create a “Do Not Track” button to allow users to quickly and easily opt out of tracking by Internet advertisers.

- Companies that commit to *Do Not Track* in their privacy codes of conduct may face FTC consequences for failure to abide by Do Not Track commitments under Section 5 enforcement proceedings (15 U.S.C. S 45).

• Despite the provision of “clearer, more understandable information to members on personal information handling practices,” on April 4, 2012, PCC cautioned that Facebook must build privacy “in at the front-end – not added after the fact in response to negative reactions from individual users and data protection authorities.”

• Google has put in place a “governance model … that ensures that necessary procedures to protect privacy are duly followed before products are launched.” In a PCC first, it has also requested that Google undergo an independent, third-party audit of its privacy programs by June 2012.
Enforcement and Remedial Approaches:

U.S. Federal Trade Commission

F.T.C. has ability to issue orders / consent decrees compelling companies to remedy their practices and follow a *Privacy by Design* approach. Companies may be compelled to ensure:

- Privacy is “baked in” as a corporate priority
- Collection of personal information is minimized
- Information handling practices are transparent
- Customers are provided with choices regarding data-related practices
Google Buzz and the F.T.C.

• April 2011 – Google settles F.T.C. deceptive privacy practice charges regarding Buzz, its social networking tool

• Terms of settlement require Google to launch a privacy program and undergo biennial third-party audits for 20 years

• The settlement does not impose a fine, but Google could face fines if it violates the terms of the settlement

• First time the F.T.C. has ordered a company to implement a comprehensive security policy
Facebook and the F.T.C.

- December 2011 – Facebook settled F.T.C. charges that it had deceived consumers by telling them they could keep their information on Facebook private, while repeatedly allowing it to be shared and made public.

- The terms of settlement require Facebook to:
  - Obtain consumers’ affirmative, express consent before enacting changes that exceed their privacy settings.
  - Undergo third-party biennial audits for a period of 20 years.

- The settlement does not impose a fine, but Facebook could face additional charges if it violates the terms of the settlement, including engaging in deceptive practices.
Conclusions

• Growing need for principled and pragmatic solutions that leverage Privacy by Design
• Recommended approach -- Embed PbD into policy, regulations, voluntary codes and best practices
• Beyond legal compliance and minimum standards is a new way to achieve privacy protection
• PbD is becoming part of a second generation regulatory framework
Resources:

- www.privacybydesign.ca
- www.realprivacy.ca
- www.ipc.on.ca
How to Contact Us

Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca
david.goodis@ipc.on.ca
stephen.mccammon@ipc.on.ca