Privacy Forms the Foundation of Freedom and Liberty

Ann Cavoukian, Ph.D.
Executive Director
Privacy and Big Data Institute
Ryerson University

World Jurist Association
Barcelona, Spain
May, 2016
Let’s Dispel Some Myths
Privacy ≠ Secrecy

Privacy is *not* about having something to hide
Privacy = Control
Privacy = Personal Control

• User control is critical
• Freedom of choice
• Informational self-determination

Context is key!
Privacy is Essential to Freedom: A Necessary Condition for Societal Prosperity and Well-Being

• Innovation, creativity, and the resultant prosperity of a society requires freedom;

• Privacy is the essence of freedom: Without privacy, individual human rights, property rights and civil liberties – the conceptual engines of innovation and creativity, could not exist in a meaningful manner;

• Surveillance is the antithesis of privacy: A negative consequence of surveillance is the usurpation of a person’s limited cognitive bandwidth, away from innovation and creativity.
The Decade of Privacy by Design
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
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.*
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Dutch</td>
<td>20. Maltese</td>
<td>33. Lithuanian</td>
</tr>
<tr>
<td>8. Estonian</td>
<td>21. Greek</td>
<td>34. Farsi</td>
</tr>
<tr>
<td>13. Arabic</td>
<td>26. Turkish</td>
<td></td>
</tr>
</tbody>
</table>
Positive-Sum Model: The Power of “And”

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 “vs.” with “and”
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**.
9 PbD Application Areas

- CCTV/Surveillance cameras in mass transit systems;
- Biometrics used in casinos and gaming facilities;
- Smart Meters and the Smart Grid;
- Mobile Communications;
- Near Field Communications;
- RFIDs and sensor technologies;
- Redesigning IP Geolocation;
- Remote Home Health Care;
- Big Data and Data Analytics.
Cost of Taking the Reactive Approach to Privacy Breaches

Proactive

Reactive

Class-Action Lawsuits
Damage to One’s Brand

Loss of Consumer Confidence and Trust
“Privacy by Design is considered one of the most important concepts by members of the Japanese Information Processing Development Center …

We have heard from Japan’s private sector companies that we need to insist on the principle of Positive-Sum, not Zero-Sum and become enlightened with Privacy by Design.”

— Tamotsu Nomura, Japan Information Processing Development Center, May 28, 2014
Recent Developments
There is widespread concern about surveillance by both government and business:

- 91% of adults agree that consumers have lost control over their personal information;
- 80% of social network users are concerned about third parties accessing their data;
- 80% of adults agree that Americans should be concerned about government surveillance;
Pew Research Internet Project (Cont’d)

– Most Americans are aware of the government’s monitoring of communications;
  • Only 5% have heard “nothing at all” about government surveillance;

– There is little confidence in the security of common communications channels;
  • 81% feel “not very” or “not at all secure” using social media to share private information.
2014 Survey of Canadians on Privacy
Office of the Privacy Commissioner of Canada

• 90% of Canadians expressed concern about the protection of their privacy;
• 78% feel at least somewhat likely that their privacy may be breached by someone using their Credit/Debit Card or stealing their identity;
• 70% of Canadians are concerned about the use of genetic testing for non-medical purposes;
• 73% feel they have less protection of their personal information than ten years ago;
• 60% have little expectation of privacy because there are so many ways it can be compromised.
Trends and Challenges: An Epidemic of Breaches

• From 2005 to 2013, there were 4,167 reported breaches involving 663,587,386 individual records;
• 30% of those whose records are breached will become victims of identity theft.

— Privacy Rights Clearinghouse

• The average cost of breach per record/individual in 2013: $201

— Ponemon Institute

“Data breaches are a fact of life in the United States.”

— Mallory Duncan,
Vice President, National Retail Federation
EU Article 29 Working Party

• Recommendations on the Internet of Things:
  – Make privacy the default setting ... follow Privacy by Design;
  – Delete all raw data after processing;
  – Respect a user’s self-determination over their own data, and seek consent in a user-friendly way;
  – Be transparent about how a user’s data is being used;
  – When sensors are continuously collecting one’s personal data, remind users of this surveillance activity;
  – Ensure that data published to social platforms remain private, by default;
  – Users should not be penalized for failing to consent;
  – Data should be De-Identified, except when necessary.
Privacy Commissioners Declaration

36th Int’l Conference of Data Protection and Privacy Commissioners on the Internet of Things

– The value of Internet of Things (IoT) is not only in the devices, but in the services that arise from their use;
– Connectivity is ubiquitous: it is the joint responsibility of all actors to ensure trust in connected systems: Transparency is Key;
– Protection should begin from the moment data that is collected;
  • “Privacy by Design should be the key selling point of innovative technologies”
– Strong, active and constructive debate is necessary to overcome the huge challenges presented by the developers of IoT.

-September, 2014
Mauritius
“The Court of Justice of the European Union (CJEU) has in its decision today declared that transfers of personal data from the EU to the US cannot rely on the Safe Harbor framework agreement.”
GDPR

General Data Protection Regulation

– Strengthens and unifies data protection for individuals within the European Union
– Gives citizens control over their personal data and simplifies regulations across the EU by unifying regulations

• Proposed – January 25th 2012
• Passed - December 17, 2015
• Adoption – Spring 2016
• Enforcement – Spring 2018
E.U. General Data Protection Regulation

• The language of “Privacy/Data Protection by Design” and “Privacy as the Default” will now be appearing for the first time in a privacy statute, that was recently passed in the E.U.

  – Privacy by Design
  – Data Protection by Design
  – Privacy as the Default
The Similarities Between PbD and the GDPR

“Developed by former Ont. Information & Privacy Commissioner, Ann Cavoukian, Privacy by Design has had a large influence on security experts, policy markers, and regulators ... The EU likes PbD ... it’s referenced heavily in Article 23, and in many other places in the new regulation. It’s not too much of a stretch to say that if you implement PbD, you’ve mastered the GDPR.”
Concluding Thoughts

• Privacy risks are best managed by proactively embedding the principles of Privacy by Design – prevent the harm from arising – avoid the data breach;

• Focus on prevention: It is much easier and far more cost-effective to build in privacy, up-front, rather than after-the-fact;

• Abandon zero-sum thinking – embrace doubly-enabling systems: Big Data and Big Privacy: Yes, we can;

• Get smart – lead with Privacy – by Design, not privacy by chance or, worse, Privacy by Disaster!
Ann Cavoukian, Ph.D.
Executive Director
Privacy and Big Data Institute
Ryerson University

285 Victoria Street
Toronto, Ontario
M5B 2K3

Phone: (416) 979-5000 ext. 3138
ann.cavoukian@ryerson.ca