



Who We Are

Commissioner Ann Cavoukian, Ph.D.:

- appointed by Ontario legislature
- independent from government
- oversees 3 privacy & access to information laws

Mandated to:

- investigate privacy complaints
- resolve appeals from refusals to provide access to information
- ensure organizations comply with the access and privacy provisions of the *Acts*
- educate public about Ontario's access and privacy laws
- conduct research on access and privacy issues, provide advice and comment on proposed government legislation & programs.



Some 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.



Principles of Fair Information Practices: → Meta Principles

<ul style="list-style-type: none">• Safeguards	Safeguards
<ul style="list-style-type: none">• Purpose Specification• Collection Limitation• Use, Retention and Disclosure Limitation	Data Minimization
<ul style="list-style-type: none">• Consent• Accuracy• Access• Redress	User Participation
<ul style="list-style-type: none">• Accountability• Openness• Compliance	Accountability (beyond data subject)



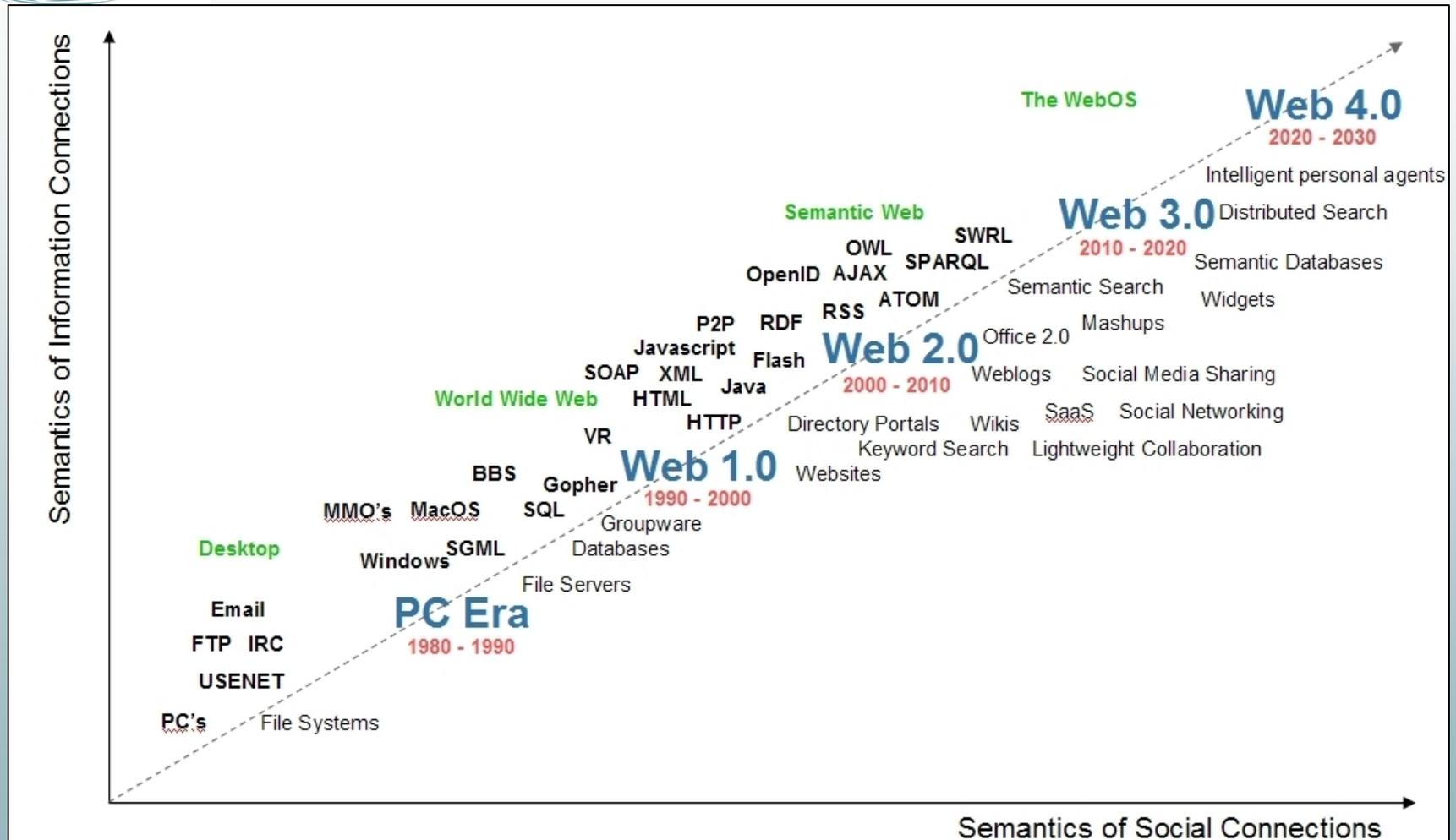
Applying privacy to information technologies and systems



- ii **Minimize collection, use, sharing, and retention of PII**
(e.g., limiting purposes, collection, use, disclosure, and retention)
- ii **Enhance data security**
(e.g., appropriate safeguards)
- ii **Actively engage the individual in managing and controlling their PII**
(e.g., consent, accuracy, access, challenging compliance, etc.)



From PC to Web 4.0



Radar Networks & Nova Spivack, 2007 – www.radarnetworks.com
www.PrivacybyDesign.ca



Challenges to Privacy

- Jurisdiction
- Technological sophistication
- Network and process complexity
- Accountability and compliance
- Preventing privacy harms



DPA Responses

- Develop independent technology evaluation capacity (e.g. IPC, Schleswig-Holstein *et alia*)
- Join Clubs (IWGDPT, ICDPPC, Art 29 WP, GPEN, etc.)
- Liaison and Standardization work (APEC, OECD, ISO, IETF, etc.)
- Advocacy (int'l Resolutions, Opinions, submissions)



Datenschutz Schleswig-Holstein

Projects:

- EuroPriSe – European Privacy Seal
- PrimeLife – Privacy & Identity Management for Europe
- TClouds – Trustworthy Clouds Privacy and Resilience for Internet-scale Critical Infrastructure
- ABC4Trust – Attribute-based Credentials for Trust
- SSEDIC – Scoping the Single European Digital Identity Community
- BEST Network - Biometric European Stakeholder Network



IWGDPT

Int'l Working Group on Data Protection in Telecommunications

- Mobile processing of Personal Data and Security
- Use of Deep Packet Inspection for Marketing Purposes
- Report and Guidance on Privacy in Social Network Services
– “Rome Memorandum”
- Trusted Computing, Associated Digital Rights Management Technologies, and Privacy - Some issues for governments and software developers
- Privacy and Security in Internet Telephony (VoIP)
- Means and Procedures to Combat Cyber-Fraud in a Privacy-Friendly Way
- Potential privacy risks associated with wireless networks
– Main Recommendations
- on a future ISO privacy standard
- on Telecommunications Surveillance
- Use of unique identifiers in telecommunication terminal equipments:
the example of Ipv6

Source: <http://tinyurl.com/4yayg8h>



ICDPPC

Int'l Conference of Data Protection and Privacy Commissioners Resolutions

2010 - Jerusalem

- Resolution on Privacy by Design

2009 - Madrid

- International Standards to Protect Personal Data and Privacy
- Observer representation before the IGF and ICANN

2008 - Strasbourg

- Resolution on a Joint Proposal for Setting International Standards on Privacy and Personal Data Protection
- Resolution to Establish a Steering Group on Representation at Meetings of International Organizations



ICDPPC

2007 - Montreal

- Resolution on International Cooperation
- Resolution on Development of International Standards

2006 - London

- London Declaration

2005 - Montreux

- Declaration of Montreux: "The Protection of Personal Data and Privacy in a Globalized World: A Universal Right Respecting Diversities"

2004 - Wroclaw

- Resolution on a Draft ISO Privacy Framework Standard

2003 - Sydney

- Resolution on Data Protection and International Organizations

Source: <http://tinyurl.com/3vgaphj>



Article 29 Data Protection Working Party

- Established by Article 29 of Directive 95/46/EC
- Independent EU Advisory Body on Data Protection/Privacy
- Primary Objectives:
 - Provide expert opinion from member state level to the Commission on questions of data protection.
 - Promote the uniform application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities.
 - Advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy.
 - Make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.



Article 29 Data Protection Working Party

Documents Adopted (selected):

- Recommendation on the respect of privacy in the context of interception of telecommunications
- Opinion on "Creating a safer information society by improving the security of information infrastructures and combating computer-related crime"
- Opinion on the use of unique identifiers in telecoms terminal equipments: the example of IPV6
- Opinion on the storage of traffic data for billing purposes
- Opinion on the use of location data with a view to providing value-added services
- Opinion on Geolocation services on smart mobile devices



Article 29 Data Protection Working Party

- Recommendation: Report and Guidance by the International Working Group on Data Protection in Telecommunications ("Budapest - Berlin Memorandum on Privacy on the Internet")
- Recommendation: Anonymity on the Internet
- Recommendation: Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware
- Recommendation: preservation of traffic data by Internet Service Providers for law enforcement purposes
- Working document "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection
- Working Document on on-line authentication services
- Opinion on the application of the data protection principles to the Whois directories

Source: <http://tinyurl.com/42x4lo2>



Adoption of “Privacy by Design” Resolution

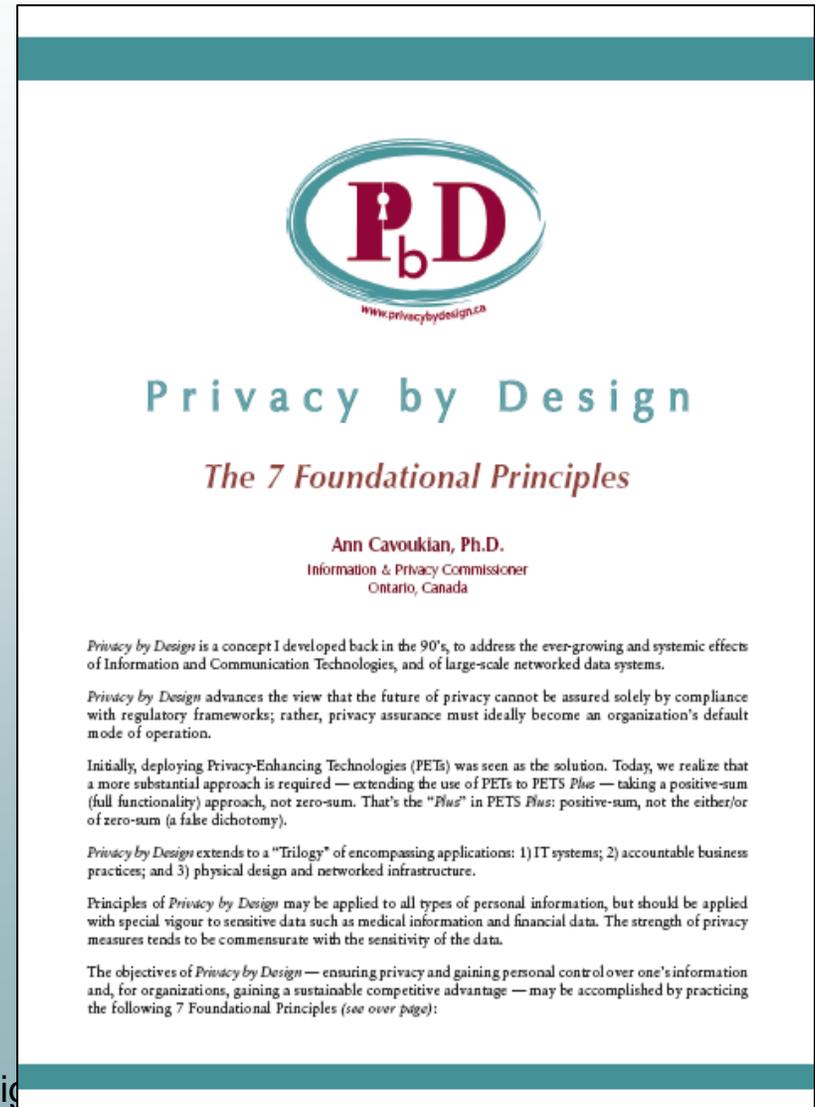
- **October 29, 2010** – regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection:
 - Encourage the adoption of the principles of *PbD* as part of an organization’s **default** mode of operation;
 - Invite Data Protection and Privacy Commissioners to promote *PbD*, foster the incorporation of its *7 Foundational Principles* in privacy policy and legislation in their respective jurisdictions, and encourage research into *PbD*.



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.PrivacybyDesign.ca

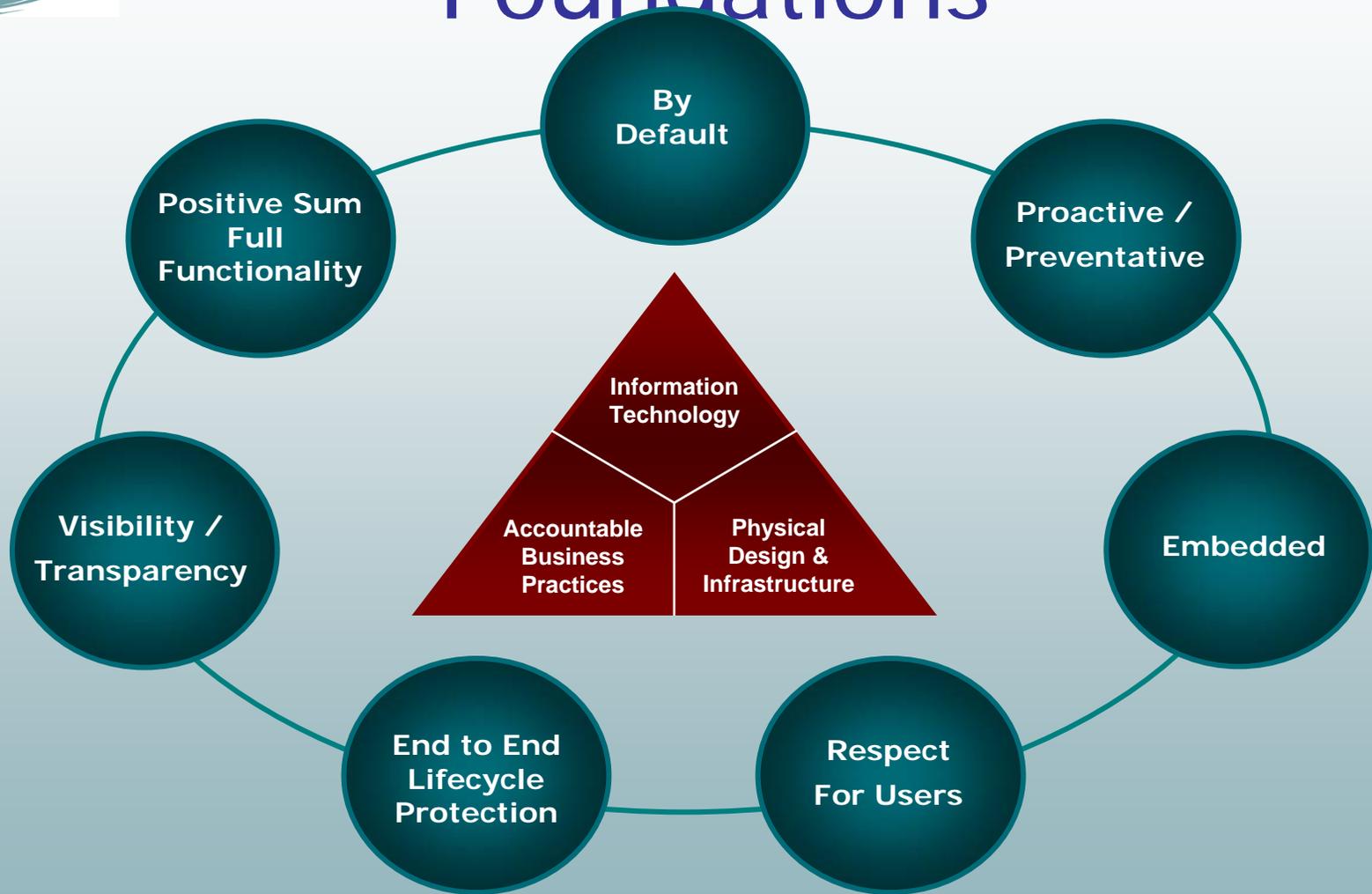


www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf



Privacy by Design Foundations

www.privacybydesign.ca





Message from Commissioner Ann Cavoukian, Ph.D.



www.PrivacybyDesign.ca



Meta-FIPs → PbD

Safeguards	End to End Lifecycle Protection
Data Minimization	Privacy as the Default (Setting)
User Participation	Respect for User Privacy
Accountability	Openness & Transparency
Leadership & Goal-Setting	Proactive Not Reaction; Preventative Not Remedial
Verifiable Methods	Privacy Embedded into Design
Quantitative Results	Full Functionality – Positive-Sum, not Zero-Sum



Privacy by Design

- Broad, universal framework
- Applies to technologies, operations/processes, and networks/architectures/eco-systems.
- Beyond FIPs (+ Leadership + Methodology + Results)
- Closest Proxies: PIA and Risk Management methods

Privacy by Design: Recognition

- US DoC paper, FTC Staff report, Kerry-McCain bill, Buzz Consent Decree, *et alia*
- EU Reform of Privacy Directive; implementation of e-Privacy directive; RFID PIA and Smart Grid initiatives



Conclusions

- DPAs are attentive and engaged, but are only part of the solution
- International coordination and high-level standardization are underway
- Much collaboration and learning required among all stakeholders
- Privacy by Design is gaining ground as a high level normative framework / approach
- Work needed now to “operationalize” PbD and apply to information infrastructures, networked eco-systems and related engineering standards and protocols.



How to Contact Us

Fred Carter

**Senior Policy & Technology Advisor
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: firstname.lastname@ipc.on.ca