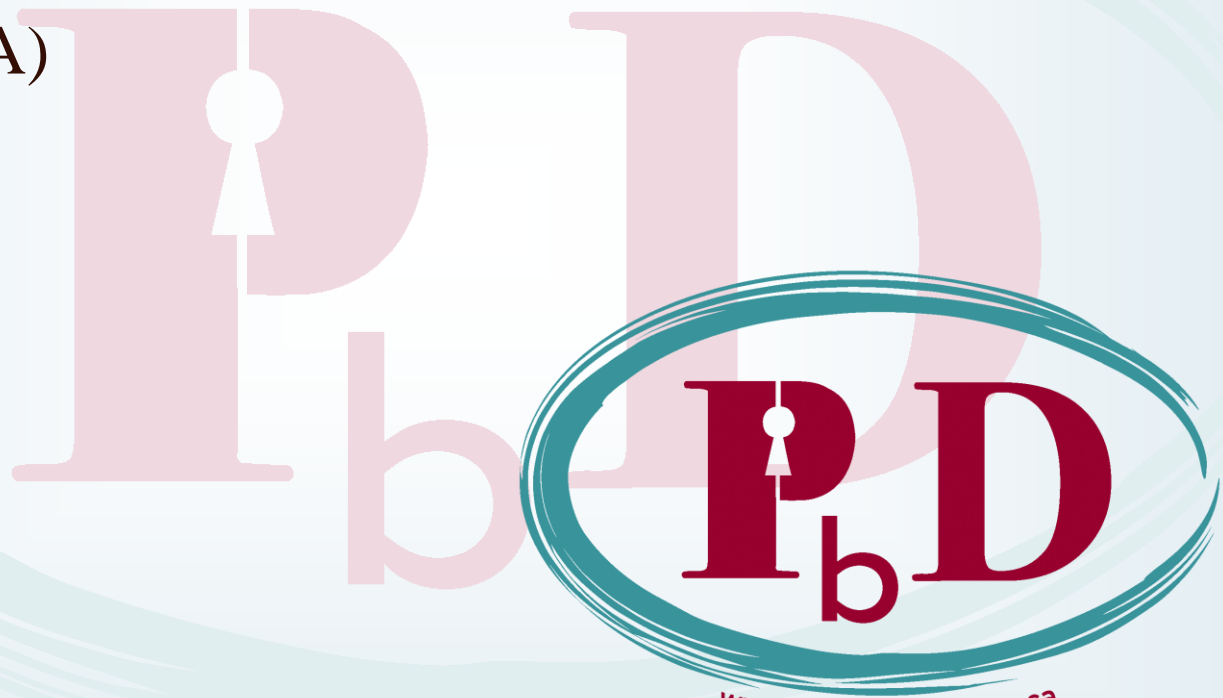


The *Privacy by Design* Privacy Impact Assessment

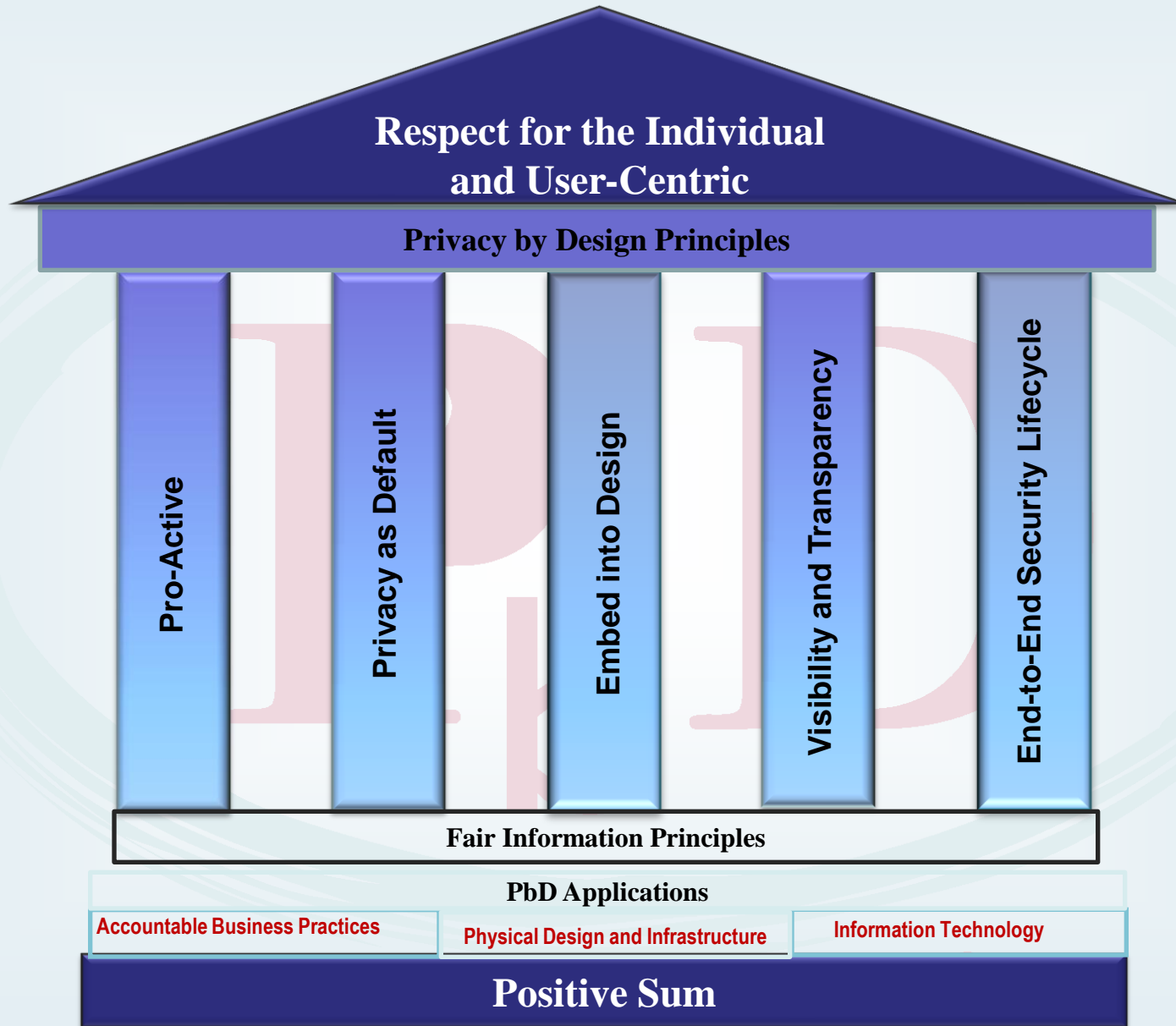
(The *PbD* PIA)



www.privacybydesign.ca

www.privacybydesign.ca

Privacy by Design Privacy Impact Assessment



Context for PbD PIA

- Approach applies to both private and public sectors
- Describes the program or technology and its privacy environment
- Identifies privacy risks, and proposes mitigating recommendations
- Focuses on the individual as the driver
- Ensures end result is always ‘positive sum’
- Takes into consideration local privacy environment and expectations of individuals
- Significance of each of the three PbD applications varies relative to each PbD Principle
- The seven PbD principles and three PbD applications are built upon the 10 Fair Information Principles – mutually inclusive

Distinguishing Features of the PbD PIA

- Based on original PbD concept and principles developed by Dr. Ann Cavoukian, Information and Privacy Commissioner/ Ontario
- Takes a holistic approach to privacy assessment
- Assesses business and cultural environments into which the program/IT solution is introduced
- Considers the privacy expectations of individuals/users regarding their personal information
- Clearly assesses privacy and security-enhancing functionality for IT solutions
- Includes a comprehensive assessment of governance of, and accountability for, personal information
- Assesses Privacy and Security in tandem throughout analysis process
- Methodology may be applied at all stages of a program /IT solution lifecycle: conceptual, physical design, and re-design

www.privacybydesign.ca

Pro-Active anticipation of privacy risks, taking into consideration the local privacy environment and the expectations of the individual

Respect for the Individual and User-Centric

Information Technology

1. Develop Privacy Architecture
2. Document Privacy business requirements for IT solutions (e.g., audit logging, reporting and alerting, consent management, access control)
3. Identify Privacy Enhancing Technologies for implementation

Accountable Business Practices

1. Assess current privacy posture (10 FIPs as framework for analysis) via Conceptual and Design/ Physical PIA
 - Policies and Procedures (breach, CUD, complaint, access and correction)
 - Governance and data stewardship
 - Accountability: agreements, assignment of accountable person
 - Review of data to be CUD and shared, and process mapping
 - Privacy and security awareness and training for staff and users
 - Assignment of, follow-through on, risk mitigation recommendations
2. Consider statutory requirements
3. Consider privacy standards and best practices
4. Monitor Compliance

Physical Design and Networked Infrastructure

1. Assess current security posture as component of PIA (using ISO standards and/or best practices as the metric)
2. Complete Conceptual and Design TRA

Positive Sum

Privacy as the Default

FIPs: 2) Identify Purposes; 3) Consent; 4/5) Limit Collection, Use, Disclosure, Retention

Respect for the Individual and User-Centric

Information Technology

1. Document Privacy and Security business requirements for IT solutions (e.g., audit logging and reporting and alerting, consent management, access control)
2. Identify Privacy Enhancing Technologies for implementation

Accountable Business Practices

Establish:

1. Privacy and Security policies and procedures
2. Agreements with vendors, agents, and partners
3. End-to-end data lifecycle, limiting collection, use, disclosure and retention
4. Staff/user privacy and security awareness and training program
5. Compliance monitoring program (internal and external)
6. Accountable person and governance structure
7. Privacy Impact Assessments
8. Public communications
9. Consent for 'opt-in' or 'opt-out'

Physical Design and Networked Infrastructure

1. Document privacy protections in physical design of data collection, access, and use at points-of-service.

Positive Sum

www.privacybydesign.ca

Embed into Design

All 10 Fair Information Principles

Respect for the Individual and User-Centric

Information Technology

1. Document Privacy and Security architecture
2. Document Privacy and Security business requirements for IT solutions (e.g., audit logging and reporting and alerting, consent management, access control)
3. Establish security standards for physical and technical environments

Accountable Business Practices

- Develop privacy policies and procedures that address:
1. Statutory requirements
 2. Fair Information Principles:
 - Accountability and governance (incl. training)
 - Identify purposes for collection, use, disclosure
 - Obtain consent
 - Limit collection of PI/PHI
 - Limit use, disclosure and retention of PI/PHI
 - Ensure appropriate accuracy of PI/PHI
 - Implement appropriate security safeguards
 - Publicly communicate information management practices
 - Provide individuals with access to, and correction of their PI/PHI
 3. Provide for lodging of complaints about privacy practices
 4. Monitor compliance
 5. Establish agreements for agents, vendors, partners

Physical Design and Networked Infrastructure

1. Implement privacy and security policies and procedures
2. Complete Conceptual and Design PIA and assign accountability for addressing risk mitigation strategies
3. Complete Conceptual and Design TRA and assign accountability for addressing risk mitigation strategies

Positive Sum

End-to-End Security Lifecycle

FIP: 7) Safeguards

Respect for the Individual and User-Centric

Information Technology

1. Document Security Architecture
2. Document Security business requirements for IT solutions (e.g., audit logging and reporting and alerting, consent management, access control)
3. Establish and implement security standards for physical and technical environments
4. Conduct Vulnerability Assessment and Penetration Testing

Accountable Business Practices

1. Assess current security posture (10 FIPs as framework for analysis) via Conceptual and Design/ Physical PIA
 - Policies and Procedures (breach, CUD, complaint, access and correction, including retention and secure destruction schedule)
 - Accountability: agreements, assignment of accountable person
 - Staff and third party privacy and security awareness and training
 - Documentation of roles and responsibilities (separation of duties)
 - Assignment of, follow-through on, risk mitigation recommendations
2. Consider statutory requirements
3. Consider security standards and best practices
4. Monitor Compliance
5. Complete Conceptual and Design TRA

Physical Design and Networked Infrastructure

1. Assess current security posture as component of PIA
2. Conduct TRA (using ISO standards and/or best practices as the metric)

Positive Sum

Visibility and Transparency

FIPs: 1) Accountability; 2) Identifying Purposes; 3) Consent; 6) Accuracy; 7) Safeguards; 8) Openness; 9) Individual Access; 10) Challenging Compliance

Respect for the Individual and User-Centric

Information Technology

1. Privacy Architecture
2. Privacy business requirements for IT solutions (e.g., audit logging and reporting and alerting, consent management, access control)

Accountable Business Practices

1. Publish summaries of Conceptual and Design PIAs and TRAs
2. Publish information about:
 - Accountable/contact person
 - Information management and privacy policies and procedures
 - Statutory authority to collect, use, and disclose PI/PHI
 - Registration of a complaint, or request access to, and correction of, PI/PHI
 - Collection of consent and withdrawal of consent

Physical Design and Networked Infrastructure

1. Assess current security posture as component of PIA (using ISO standards and/or best practices as the metric)
2. Complete Conceptual and Design TRA

Positive Sum

www.privacybydesign.ca

Authors

Anita Fineberg, LL.B., CIPP/C

Barrister & Solicitor

President

Anita Fineberg & Associates Inc.

Pat Jeselon, MBA, CMC

President

Pat Jeselon & Associates Consulting Inc.

www.privacybydesign.ca