

A Foundational Framework for a *PbD* – PIA

November 1, 2011



Pat Jeselon, MBA, CMC
Health Information Privacy Consultant



Pat Jeselon & Associates Consulting Inc.

Privacy by Design Ambassador
Toronto, Ontario

Anita Fineberg, LL.B., CIPP/C
Barrister & Solicitor

Anita Fineberg & Associates Inc.

Privacy By Design Ambassador
Toronto, Ontario

Table of Contents

- 1 FOREWORD 1**
- 2 INTRODUCTION 2**
 - 2.1 PURPOSE OF THIS FRAMEWORK 3
 - 2.2 SCOPE OF THE FRAMEWORK 4
 - 2.3 OUT-OF-SCOPE 4
- 3 THE SEVEN *PBD* PRINCIPLES..... 5**
 - 3.1 CONTEXT FOR THE FRAMEWORK 7
- 4 THE FRAMEWORK 9**
 - 4.1 UNIQUENESS OF THE FRAMEWORK 9
 - 4.2 THE LIFE CYCLE OF THE FRAMEWORK 9
- 5 USING THE FRAMEWORK 11**
 - 5.1 HOW TO USE THIS FRAMEWORK 11
 - 5.2 APPLICATIONS OF THE FRAMEWORK..... 12
- 6 CONCLUSION 25**
- 7 SOURCES 26**

1 Foreword

The past twelve months have marked a period of unprecedented growth in the application of the Principles of *Privacy by Design*. It has been embraced by the European Commission, the U.S. Federal Trade Commission and, significantly, has been unanimously adopted as an International Standard by Data Protection Authorities and Privacy Commissioners. It is not surprising that *Forbes* recently proclaimed that “*Privacy by Design* is the New Corporate Hotness.”

Privacy by Design (PbD) represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices and providing remedies for privacy breaches, after-the-fact. Advocating privacy as a core requirement of systems, right from the outset, it is a proactive approach to privacy protection which seeks to *avoid* data breaches and their attendant harm. In the case of existing and legacy systems, the approach has been extended further and is called *Privacy by ReDesign*. *PbRD* offers a transformative framework for undertaking a proactive assessment of existing gaps in how personal information is managed, and addresses those gaps systematically. Both approaches emphasize positive-sum solutions with win-win outcomes.

As organizations work to apply the 7 Foundational Principles of *PbD*, they increasingly seek guidance regarding practical issues of implementation. Focused as it is on the Privacy Impact Assessment (PIA), an essential tool in the privacy professional’s toolbox; this guide to *A Foundational Framework for a PbD-PIA* is especially timely.

The guide emphasizes what most now accept as a best practice, the continuous use of the PIA throughout the systems development process – from project inception to implementation. Posing questions specifically associated with fulfilling each of the Principles, it is a framework which addresses the needs of organizations with modest personal information protection requirements. Its potential to augment and complement existing PIA processes, however, is truly valuable.

I am grateful to the paper’s authors, Anita Fineberg and Pat Jeselon, both of whom are highly respected colleagues. Recognizing the need for such a paper, these committed professionals volunteered to share their knowledge of the area and help fill a void in the growing body of work describing the application of *PbD*.

I encourage you to read and consider the framework presented in this guide. Use it, test it and share your experiences on the Forum at www.privacybydesign.ca. Working together, we can ensure that the practice of building privacy into systems becomes as natural as satisfying any other business requirement. The future demands no less.

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner
Ontario, Canada

November, 2011

2 Introduction

In the 1990s, Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, developed the concept *Privacy by Design (PbD)*. *PbD* describes the philosophy of embedding privacy from the outset into the design specifications of information technologies, accountable business processes, physical spaces, and networked infrastructures ('the Applications'). *PbD* represents a proactive, holistic approach to protecting the privacy of individuals, rather than the reactive approach associated with traditional privacy frameworks that focus on minimum standards for information practices and remedies for privacy breaches after breaches have occurred and the harm has been done.

Since its initial development, *PbD* has gained traction among policy makers, regulators, and decision makers around the globe.¹ At the thirty-second Annual International Conference of Data Protection and Privacy Commissioners, Dr. Cavoukian proposed a *PbD* Resolution² that was unanimously passed and adopted. Considered a 'landmark resolution,' the Conference recognized *PbD* as an essential component of fundamental privacy protection.

With the rapid pace of technological change, the protection of an individual's privacy cannot be assured solely by compliance with currently existing regulatory frameworks. In the face of class action litigation and front-page adverse publicity resulting from privacy breaches, organizations can no longer afford to turn a deaf ear and a blind eye to the environment of client expectations—legal compliance alone is no longer sufficient. It is, therefore, no surprise that there is increasing momentum behind *PbD* as "the new generation of privacy protection."³

The current challenge is to convert the momentum behind the philosophy of *PbD* into practical approaches to incorporating *PbD* into organizational practices; that is, to determine how to make *PbD* operational. In her recent paper, *Privacy by Design in Law, Policy and Practice*,⁴ Dr. Cavoukian identified nine approaches to the adoption of *PbD* by an individual organization.⁵ She noted that while a privacy impact assessment (PIA) "can be an excellent entry point for applying the principles of *Privacy by Design*, [privacy impact assessments] are not generally grounded in the seven Principles of *Privacy by Design*," and called for more work to be completed in this area.⁶

¹ Cavoukian, Ann, PH.D., Information & Privacy Commissioner, Ontario Canada, *Privacy by Design in Law, Policy and Practice*, a White Paper for Regulators, Decision-makers and Policy-makers (August 2011), provides an excellent summary of the significant developments in the area, <http://www.ipc.on.ca>

² <http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf>

³ *Ibid.*, at p.3.

⁴ Fn.1.

⁵ These approaches are: PIAs, Risk Analysis, Gap Analysis, Threat Assessment, Employee Training Tools, Privacy Risk Management, Audits, Certification and Seals.

⁶ Fn.1, at p. 15.

2.1 Purpose of this Framework

The purpose of this Foundational Framework for a *PbD* Privacy Impact Assessment (the ‘Framework’) is to answer the Commissioner’s call and provide organizations with a practical tool to direct and inform decisions in the design of an information technology, business process, physical space and networked infrastructure to ensure that both privacy and ‘business’ functionality are built in from the outset. The Framework takes into consideration consumer privacy expectations and is applicable in both private and public sector environments. This Framework may be used by all organizations that collect, use, disclose, transfer, retain, and dispose of Personal Information (PI), regardless of the industry, or where they are located in the world.

With its focus on respect for the individual, and a user-centric approach, the Framework is intended to guide organizations towards achieving a positive-sum outcome, a win-win solution for both their customers and their businesses, by ensuring the protection of an individual’s privacy without sacrificing functionality or security. Whenever the *PbD* Principles are applied, the result is a more meaningful understanding of privacy across the organization.

This Framework does not replace or negate the need for organizations to ensure that their privacy practices and controls meet local legislative and/or regulatory requirements. While the Framework incorporates Fair Information Principles (FIPs) as the minimum basis for privacy analysis,⁷ organizations must customize the Framework to include both local legal and environmental privacy considerations. By adopting this approach, organizations will have a single tool that captures the full spectrum of privacy issues that should be addressed in the development of the Applications.

The following were taken into account in developing the Framework:

- There is a need for both privacy and business professionals to consider privacy in a holistic manner;
- *PbD*, which embraces and extends the FIPs, is an approach that enables organizations to achieve this goal;
- Legislative compliance is a necessary, but not a sufficient, condition to ensure appropriate privacy protection;
- The Framework should be supplemented by industry-specific questions, jurisdictionally-specific legislative requirements, as well as considerations related to the environment in which the organization operates;
- Privacy professionals should consider using this Framework to augment PIAs based on a compliance/regulatory approach; and
- The Framework should also provide a useful baseline for anyone concerned about delivering privacy protective Applications following the *PbD* Principles.

⁷ “Privacy by Design The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices,” Dr. Ann Cavoukian, Ontario Information and Privacy Commissioner.

2.2 Scope of the Framework

The scope of the Framework is broader than other PIAs that focus primarily on an organization's compliance with legislative and regulatory requirements and FIPs⁸. *PbD* assumes a holistic approach to privacy by transforming how an organization manages the privacy of individuals from policy and compliance to an organization-wide business issue and/or strategy. *PbD* adopts a holistic approach to privacy by:

- Ensuring privacy protection is embedded into information technology, business processes, physical spaces and networked infrastructures from the outset; and
- Encouraging organizations to adopt the *PbD* Principles into all aspects of their operations wherever and whenever PI is collected, used, disclosed, retained, transferred, and/or disposed.

The Framework discusses the application of the seven *PbD* Principles in three areas:

- 1) Information technology;
- 2) Accountable business processes, and
- 3) Physical design and networked infrastructure.

2.3 Out-of-Scope

The Framework does not include discussion of local privacy drivers. As such, the Framework does not address the privacy legislation and regulatory requirements to which an organization is subject. It does require organizations to consider the political, industry, or technical environments in which the Application will operate, as well as the privacy expectations of the organization's clients and other stakeholders. However, these elements, as well as legal requirements, should be specifically tailored to the organization's unique circumstances and incorporated, where appropriate, into the Framework provided for each of the *PbD* Principles.

⁸ Includes GAPP (Generally Accepted Privacy Principles).

3 The Seven *PbD* Principles

The *PbD* Principles express a philosophy and methodology that inform the design of an organization's information technology, business processes, physical spaces and networked infrastructures. The application of the *PbD* Principles to these Applications creates an environment in which a culture of privacy can be established, where individual privacy and data protection is the 'norm' in organizational and employee attitudes and behaviours.

Section 5 of this document provides a framework against which an organization's approach to privacy protection can be assessed against the seven *PbD* Principles to establish its overall privacy posture. The seven *PbD* Principles are:

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 Life Cycle Protection**.
6. Visibility and Transparency—**Keep it Open**.
7. Respect for User Privacy—**Keep it Individual and User-Centric**.⁹

As the *PbD* Principles are the initial reference point for the Framework, they are provided below with explanatory notes.¹⁰

1. **Proactive** not Reactive—Preventative not Remedial

The *PbD* approach is characterized by proactive rather than reactive measures. The design anticipates and prevents privacy invasive events before they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred—the aim is to prevent privacy breaches from occurring. In short, *PbD* comes before-the-fact, not after-the-fact.

2. Privacy as the **Default Setting**

PbD seeks to deliver the maximum degree of privacy by ensuring that PI is automatically protected in any given Application. If an individual does nothing, his/her privacy still remains intact. No action is required on the part of individuals to protect their privacy—privacy is built into the Application by default.

⁹ The term 'User-Person' refers to an individual.

¹⁰ Cavoukian, Ann, PhD., Information & Privacy Commissioner, Ontario Canada, *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* (Originally published: May 2010, Revised January: 2011), at <http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf>.

3. Privacy **Embedded** into Design

PbD is embedded into the design and architecture of the Applications; it is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered without diminishing functionality.

4. Full Functionality—**Positive-Sum**, not Zero-Sum

PbD seeks to accommodate all legitimate interests and objectives in a positive-sum ‘win-win’ manner, avoiding unnecessary trade-offs. *PbD* avoids the pretence of false dichotomies, such as privacy vs. security. Privacy does not gain or lose at the expense of functionality and security.

5. End-to-End Security—**Full Life Cycle Protection**

PbD, embedded into the Application prior to the collection of any PI, extends throughout the entire life cycle of the PI involved. Strong security measures are an essential and necessary (but insufficient) condition to ensuring privacy. The presence of strong security controls ensures PI is protected throughout its life cycle, from the point of collection through to its secure and timely destruction.

6. Visibility and Transparency—**Keep it Open**

PbD seeks to assure stakeholders that whatever the Application involved, it is, in fact, operating according to the organization’s stated promises and objectives. An organization’s Applications must conform to its stated privacy and security practices. These practices are subject to independent verification, and are made visible and transparent to all.

7. Respect for User Privacy—**Keep it Individual Centric**

Above all, *PbD* requires architects, operators, and business analysts to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

This means that the privacy interests of the individual are paramount and kept uppermost in mind and practice through the implementation of, and compliance with, privacy practices and security protections that are embedded into an organization’s information technology, business processes, physical spaces and networked infrastructure.

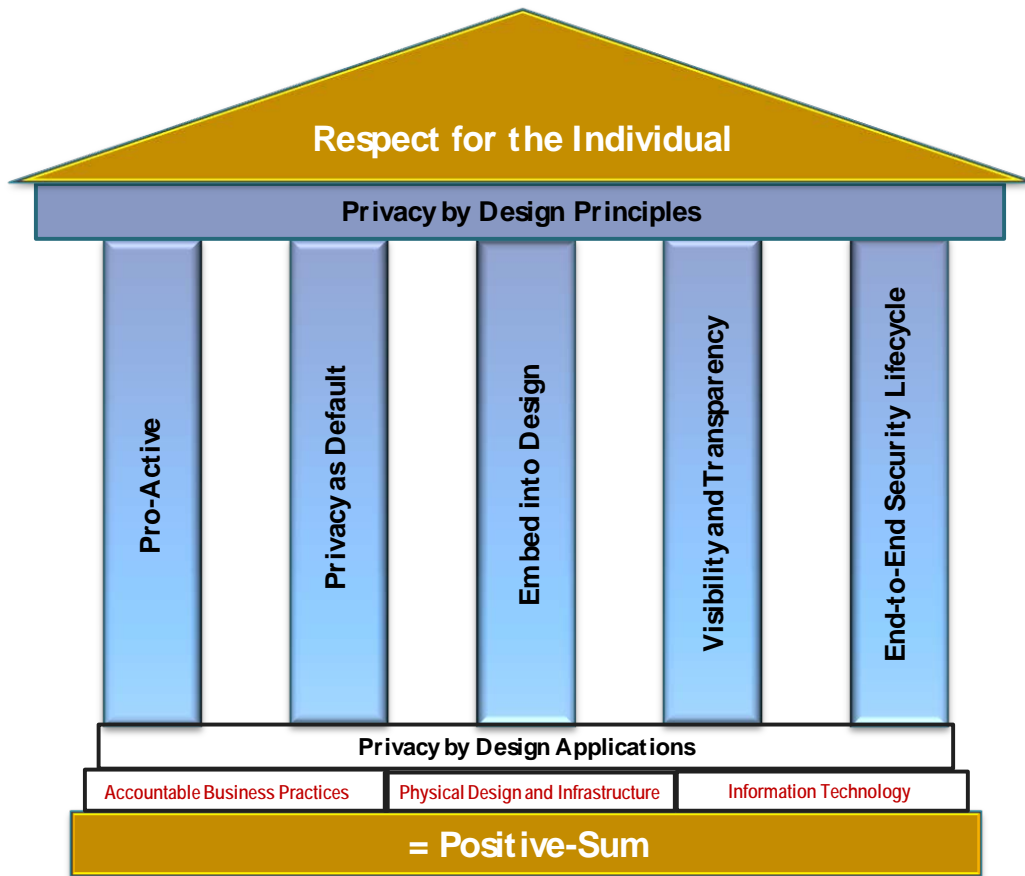


Figure 1 Framework for Privacy by Design Privacy Impact Assessment

Figure 1 presents the *PbD* Principles as Pillars, with Principle 7 at the top of the Framework to reflect the strong focus on respecting the privacy of the individual. This focus is carried into the application of the *PbD* Principles to an organization's information technology, business processes, physical spaces and networked infrastructure. The significance of an individual Principle may vary between the three Applications. The end goal is to achieve a win-win, positive-sum result where privacy does not 'win' through loss of functionality or security.

3.1 Context for the Framework

The Framework may be applied and the subsequent analysis undertaken and completed within an organization's established approach to conducting PIAs. This means that the privacy analysis should include the following:

- Description of the business purpose(s) of the Application;
- Discussion and analysis of the organization's current privacy and security policies, procedures and processes, as well as governance and accountability structures;

- End-to-end description and analysis of business processes and data flows relating to the Application, including a description of the actors involved in the collection, use, disclosure, transfer, retention, and destruction of PI;
- Detailed analysis of the Application's privacy controls (such as those for consent management, access control and audit logging/alerting/reporting, user notification);
- Detailed description and analysis of the design of the Application, including the security features or controls; and
- Identification of privacy and security risks associated with the Application, accompanied by proposed recommendations to mitigate, or eliminate, the risks.

The *PbD* Principles should be appropriately considered in each of the above analyses to ensure that a holistic approach to the analysis is taken. When applied, the Framework serves to ensure that the completed analysis captures the entire scope of an organization's privacy and data protection program, as well as the design and functionality of its information technology, business processes, physical spaces and networked infrastructure.

4 The Framework

As discussed in the preceding section, the *PbD* PIA does not necessarily replace a traditional ‘compliance-based’ PIA, or other methodologies an organization may use for conducting a privacy and data protection risk analysis. Rather, it augments such work. The Framework provides an opportunity for an organization to make certain that all necessary privacy and security controls are in place to ensure that an individual’s PI is adequately protected throughout its life cycle by applying the holistic approach of the *PbD* Principles. The *PbD* PIA can thus serve as a building block for the organization’s information governance and risk management program.

4.1 Uniqueness of the Framework

Certain unique features distinguish the Framework from the more traditional approaches of conducting a PIA. In particular, the Framework:

- Encourages organizations to take into consideration the privacy expectations of the individuals regarding their PI¹¹;
- Clearly assesses privacy and data protection practices and controls present in an organization’s information technology, business process, and physical design and networked infrastructure;
- Includes a comprehensive assessment of the governance of, and accountability for, PI by considering an organization’s privacy and data protection practices in their entirety;
- Appropriately assesses privacy and security in tandem throughout the analysis process; and
- Provides recommendations that focus on achieving a ‘positive-sum’ outcome.

4.2 The Life Cycle of the Framework

The methodology set out in this Framework should be applied continuously at all stages (conceptual, physical, and logical) of the design, development and implementation of the information technology, business process, physical space and networked infrastructure.

The methodology may also be applied to the re-design of legacy information technologies, business processes, physical spaces, and networked infrastructures.

However, applying the Framework at the outset of the design of any of the Applications allows an organization to account for costs related to privacy and security in design, development, and

¹¹ Proceeding with a new feature that is disliked by customers not only wastes ‘sunk costs’ for the initial development, but also results in potential incalculable costs related to diminished goodwill.

implementation budgets. Addressing privacy after-the-fact tends to be extremely costly, and in some instances, not practical. As a result, privacy risks may not be identified and even those risks that are identified may not be adequately mitigated.

Where an organization has not taken proactive measures to put in place practices and controls that protect the privacy of individuals with respect to their PI and to protect the confidentiality of that information, or where the organization is unable to effectively 'retro-fit' an Application, the costs stemming from a privacy breach can be significant. These costs are not limited to those associated with notification, containment, investigation and remediation of a privacy breach and the costs associated with any litigation that may arise from the privacy breach, such as legal fees. A privacy breach may also result in loss of customer/client trust and goodwill, may negatively impact stock value, and may result in damage to reputation. From the individual's perspective, privacy breaches can result in embarrassment, stigmatization, discrimination, identity theft, a loss of benefits (e.g., insurance), a loss of opportunities (e.g., a job, a promotion, housing), and other adverse consequences.

5 Using the Framework

Organizations are encouraged to customize the Framework to accommodate the specificities of their industry, as well as local business, cultural, legislative, regulatory and technical environments.

The preceding discussion established the rationale for, and context of, the *PbD* approach to conducting a PIA. This section of the Framework provides the reader with information on how to use the Framework.

5.1 How to Use this Framework

Each of the *PbD* Principles is individually addressed in the following tables through questions that the reader is asked to consider within the context of his/her industry and local environment. The scope of the questions includes all three Applications.

Following these questions, where appropriate, additional questions specific to one, or more, of the Applications are added. The relevance and/or 'weight' of each principle may vary depending on the nature of the industry or Application being analyzed. For example, providing end-to-end security, in the context of the IT Application, to ensure full life cycle protection of PI (Principle 5) is critically important to the design of an electronic medical record that provides authorized persons with access to patients' personal (health) information. The principle will be less relevant when considering a patient education program in which individuals' personal health information is used by a pharmacist to send them notices of 'Diabetes Management Days.'

Finally, the user is presented with potential benefits that may accrue to the organization as a result of conducting a *PbD* PIA, and the resulting analyses of an organization's information technology, business process, and physical design and networked infrastructure, based on the *PbD* Principles. (See Section 5, *Benefits to the Organization*.)

5.2 Applications of the Framework

The Framework begins with Principle 7 as it is this Principle that sets the tone of the privacy analysis of the organization's information technology, business process, physical space and networked infrastructure, ensuring that the privacy of the individual is protected and respected in both the identification of privacy and security risks and recommendations to mitigate the risks. In other words, this Principle relates to, and provides, the approach to the application of all of the other six Principles.

Principle 7: Respect for User Privacy: This Principle establishes the focus of the *PbD* philosophy. Above all, *PbD* requires architects and operators to keep the interests of the individual uppermost in mind by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Best *PbD* results are usually those consciously designed around the interests and needs of individuals who have the greatest vested interest in the management of their own PI.

Principle 7: Respect for User Privacy

Policies and Procedures

- a) Have you implemented policies and procedures:
 - o To ensure individuals are informed (via a public notice or other mechanism) about the purposes for the collection, use, transfer and disclosure of their PI at, or before, the time the PI is collected?
 - o To obtain the consent of individuals to the collection, use, and disclosure of their PI, where appropriate, or where otherwise required by law?
 - o For obtaining and recording consent for the collection, use, and disclosure of PI, taking account individuals' expectations and statutory or regulatory requirements?
 - o For individuals to withhold or withdraw their consent for the collection, use, and disclosure of their PI (except where otherwise permitted or required by law)?
 - o To ensure individuals may request access to, and correction of, their PI?
 - o To ensure individuals are aware of how to make a privacy complaint?
 - o To ensure individuals are aware of the redress mechanisms, including how to access the next level of redress?
 - o To ensure individuals are aware of how to contact your organization's person accountable for privacy?
- b) Are all policies, procedures, and information directed to individuals easily and freely accessible and written in easy-to-understand plain language?
- c) Are your procedures simple to use?
- d) Have you posted layered notices to enable individuals to understand your policies and procedures in more, or less, detail, as they wish?
- e) Do your notices provide individuals with adequate information about how you protect their privacy, as well as inform them of their privacy rights, including their rights to withhold or withdraw their consent to the collection, use and disclosure of their PI?
- f) Are your notices posted where they are likely to come to the attention of individuals or are individuals

Principle 7: Respect for User Privacy

provided copies of such notices?

- g) Have you implemented policies and procedures to ensure PI is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes for its collection and use?

Privacy Expectations

- h) Have you completed an assessment of the expectations of individuals with respect to the purposes for which their PI is being collected, used, and disclosed?
- i) Have you completed an assessment of the expectations of individuals with respect to the type of consent that is appropriate based on the nature of information being collected, used, and disclosed?
- j) Have the privacy and security policies and procedures of the organization been aligned with these expectations to the extent possible?

Consent

- k) Are the procedures implemented to enable individuals to consent and to withhold or withdraw such consent easy to access and use?
- l) Have mechanisms been implemented to manage individual consent, including the decision to withhold or withdraw such consent?

Principle 7: Benefits to the Organization

- a) Provides assurance to clients that your organization respects their privacy and has taken adequate steps to ensure the protection of their PI throughout its life within the organization.

Principle 1: Proactive not Reactive—The *PbD* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred—it aims to prevent privacy risks from occurring. In short, *PbD* comes before-the-fact, not after.

Principle 1: Proactive not Reactive

Accountability:

- a) Has an ‘accountable’ person been assigned responsibility for developing, maintaining, and implementing your organization’s privacy and data protection practices?
- b) Has an ‘accountable’ person been assigned responsibility for developing, maintaining, and implementing your organization’s information security program?
- c) Is there visible executive commitment to continuously set and enforce high standards of privacy and security practices?
- d) Is this commitment demonstrably shared by user communities and stakeholders?
- e) Is there a procedure in place to ensure that executives and the board of directors are regularly updated on the privacy and security program, including policies and procedures?
- f) Has a privacy and security governance and accountability framework been developed to ensure compliance with the privacy and security policies and procedures that have been implemented?
- g) Are all employees, volunteers, and contractors who access PI required to sign Confidentiality Agreements? Are they required to re-execute their Confidentiality Agreements on an on-going basis, for example, annually?
- h) Have you ensured that privacy and security protection is built into the terms of service level agreements, data sharing agreements, third party agreements, and other legal instruments?

Policies and Procedures:

- i) Have you implemented a procedure for identifying and managing privacy breaches?
- j) Have you implemented a procedure for identifying and managing information security breaches?
- k) Have you established a schedule for the on-going review of your privacy and security policies and procedures to take account of evolving privacy and security standards and best practices and statutory and regulatory changes?

Privacy and Security Risk Management:

- l) Have you implemented a Corporate Risk Management Framework?
- m) Do your project plans for the development, or redesign, of your information technology, business practices, and physical design and networked infrastructures include ‘privacy approval gateways’?¹²
- n) Is a PIA required to be conducted at the conceptual, design, logical, and redesign stages of the Application?
- o) Is the PIA reviewed and approved by senior executives of your organization?

¹² These are specific checkpoints in the project plan at which privacy issues must be analyzed and addressed before the project may proceed to the next step of development or redesign.

Principle 1: Proactive not Reactive

- p) To the extent possible, do you mitigate all of the risks identified in PIAs?
- q) Are PIAs reviewed on an on-going basis to ensure they continue to be accurate and consistent with the organization’s information practices, and to ensure that the recommendations have been, or are being, addressed by the organization?
- r) Have you established standardized methods to proactively identify and address inadequate privacy technical designs and privacy practices?

Privacy and Security Training and Awareness:

- s) Have you implemented a privacy and security awareness and training program?
- t) Are all employees, volunteers, and contractors who access PI required to attend initial privacy and security training prior to being given access to PI?
- u) Are employees, volunteers and contractors who access PI provided role-based training to understand how to apply the privacy and security policies and procedures of the organization in their daily employment, contractual or other responsibilities?
- v) Are all employees, volunteers, and contractors who access PI required to attend privacy and security training on an on-going basis (e.g., annually)?
- w) Is the privacy and security awareness and training program regularly updated as changes in the business or statutory environments require?

Audit and Compliance:

- x) Have you implemented policies and procedures to monitor, evaluate, and verify compliance with your privacy and security policies and procedures and with the terms related to privacy and security contained in agreements and other legal instruments?
- y) Do you have a mechanism for monitoring and reporting on compliance with your privacy and security policies and procedures, and the terms related to privacy and security contained in agreements and other legal instruments?
- z) Have you implemented a program of privacy and security audits?
- aa) Do you retain independent third parties to audit your organization’s practices against your privacy and security policies and procedures?
- bb) Are procedures in place to ensure that the recommendations arising out of privacy and security audits are addressed?

Information Technology	Accountable Business Processes	Physical Design and Networked Infrastructure
<ul style="list-style-type: none"> a) Have you completed a security Threat and Risk Assessment (TRA)? b) To the extent possible, have you mitigated all of 	<ul style="list-style-type: none"> a) Privacy and security policies and procedures are reviewed as part of the PIA analysis. b) Policy requires that a TRA 	<ul style="list-style-type: none"> a) Do you have a set of guidelines related to physical design and the protection of individual privacy, such as controlled

Information Technology	Accountable Business Processes	Physical Design and Networked Infrastructure
<p>the risks identified in the TRA?</p>	<p>be completed concurrently with the PIA with a focus on the physical and technical safeguards that are implemented and/or absent.</p>	<p>access to the premises and locations where PI is retained, and the incorporation of varying levels of security with each successive level being more secure and restricted to fewer individuals?</p> <p>b) Have you completed an assessment of the risks inherent in the physical design and networked infrastructure?</p> <p>c) To the extent possible, have you mitigated all of the risks identified in this assessment?</p>

Principle 1: Benefits to the Organization

- a) Supports informed decision-making and design, as well as anticipates possible privacy concerns associated with the information technology, business procedure, physical design or networked infrastructure.
- b) Considers external risk factors, such as social, legal, technological, and competitive environment, drivers, and trends in privacy issues, and the perceptions and expectations of external stakeholders regarding privacy. This consideration generates confidence that privacy objectives are being considered and addressed in the development and implementation of new systems and procedures.
- c) Ensures internal risk factors are addressed including governance, operational and strategic objectives, roles and accountabilities, policies and procedures, information systems and data flows and decision-making processes.
- d) Proactively addresses situations that, if not considered, could result in a privacy breach.

Principle 2: Privacy as the Default Setting—*PbD* seeks to deliver the maximum degree of privacy by ensuring that PI is automatically protected in any given Application. No action is required on the part of individuals to protect their privacy—privacy protection is built into the Application by default.

Principle 2: Privacy as the Default Setting

- a) Do you design information technologies, business processes, physical spaces and networked infrastructures around the principles of minimizing the identifiability, observability, and linkability of PI to the greatest degree possible?
- b) Do you ensure that the purposes for which PI is collected, used, and disclosed are clear, limited, and relevant to the circumstances?
- c) Do you ensure PI is collected, used, and disclosed according to the stated purposes for its collection, use, and disclosure?
- d) Do you collect, use, and disclose PI only if other information would not serve the purpose?
- e) Have policies and procedures been developed and implemented that require the use of encrypted, de-identified, or aggregate information, rather than PI, where PI is not necessary to serve the purpose?
- f) Do these policies and procedures require the encryption of all PI collected, used, and disclosed using mobile devices?
- g) Do you collect, use, and disclose the minimum amount of PI necessary to serve the purpose?
- h) Are the categories of PI that are being collected reviewed on an on-going basis to ensure the collection of PI is limited to that which is required to fulfill the purposes for which it is collected?
- i) Have you determined that your collection of PI is fair and necessary for a lawful purpose?
- j) Are procedures in place to review de-identified and aggregate information prior to its use or disclosure to ensure the information does not identify an individual, and that it is not reasonably foreseeable that the information could be used to identify an individual?
- k) Have you implemented user access controls based on ‘need to know,’ and ‘least privilege’ principles? Does access control extend to technical staff?
- l) Do you ensure that if individuals take no action to protect their privacy, their privacy is nonetheless still protected?

Information Technology	Accountable Business Processes	Physical Design and Networked Infrastructure
<ul style="list-style-type: none"> a) Have policies and procedures been developed to outline the acceptable use of information technologies? 		

Principle 2: Benefits to the Organization

- a) Reassures the individual whose PI is being collected, used, and disclosed that appropriate privacy controls and practices were implemented.
- b) Ensures individuals are made aware of their privacy rights and how they can exercise them, which, in turn, builds trust.

Principle 3: Privacy Embedded into Design: *PbD* is embedded into the design and architecture of IT systems, business practices, and physical design and networked infrastructures. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

Principle 3: Privacy Embedded into Design

Privacy and Security Program:

- a) Have you ensured your privacy and security program, and its associated policies and procedures, meet or exceed industry-accepted standards, frameworks, models, best practices, and guidelines, in addition to statutory requirements?
- b) Have privacy and security controls been developed and implemented in a manner that, to the extent possible, minimizes the risk of theft, loss, and unauthorized use or disclosure of PI?
- c) Are your privacy and security controls amenable to external reviews/audits?

Privacy and Security Architecture:

- d) Have you documented and distributed a Privacy Architecture for your organization to ensure established privacy protections are built into the design of all Applications that collect, use, and disclose PI? Does your Privacy Architecture:
 - o Ensure FIPS are built into the design or redesign of the Application;
 - o Classify data in terms of its level of identifiability and its sensitivity;
 - o Include a Glossary of Privacy Terminology to explain the meaning of the terms used in the documentation used by the organization;
 - o Impose restrictions on collection, use, and disclosure of PI;
 - o Limit the secondary uses of PI;
 - o Impose requirements for the use of encrypted, de-identified and aggregate information instead of PI, whenever possible; and
 - o Set out business rules for consent management, access control, audit logging, reporting and alerting, **user**-notification, and individuals access to, and correction of, their PI?
- e) Have you documented and distributed a Security Architecture to ensure established security safeguards (administrative, physical, and technical) are built into all Applications that collect, use, disclose, and retain PI?
- f) Have you implemented procedures and/or mechanisms to verify that the privacy and security architectural requirements have been appropriately designed into the functionality of the Application? Do they include 'privacy and security review and approval gateways' throughout the design, development, and redesign processes?
- g) Have you implemented user access controls based on 'need to know' and 'least privilege' principles?

Principle 3: Privacy Embedded into Design

Design Requirements for the Application:

- h) Do you have a defined process for the design and redesign of any new IT systems, business practices, and physical design and networked infrastructures that must be followed and approved by the individual(s) responsible for privacy and security in the organization prior to it being implemented?
- i) Is this process documented and distributed to all individuals within the organization responsible for the design or redesign of such Applications?
- j) Do you conduct audits to ensure that this process is consistently applied?
- k) Does this process include the following elements:
 - o Consultations in the design or redesign stages of an Application with those internal and external to the organization who will be collecting, using, or disclosing PI?
 - o Conducting PIAs and TRAs at the conceptual, physical, logical, and redesign stages of the Application?
 - o Procedure to manage and address risks identified in such PIAs and TRAs prior to the implementation of the specific Application?
 - o Ensuring PIAs and TRAs include the choices for remediation of privacy and security risks and the reasons those choices were made?
 - o Requirement that, where possible, privacy enhancing technologies appropriate to the Application and the sensitivity of the PI that is collected, used, or disclosed, such as strong encryption or de-identification, are incorporated into the design or redesign?
 - o Requirement to ensure that PI is required for purposes of the Application and that only the minimum amount of PI is collected, used, or disclosed in the Application?
 - o Incorporation of the privacy and security requirements into any Requests for Proposals issued by the organization in the event that the Application is to be built and implemented by a third party?
 - o Access controls and requirements for authentication and identification of individuals who will have access to the PI in the Application, and a mechanism for auditing such access?
 - o Establishment of rules to identify the individuals who require access to the PI based on 'need to know' and 'least privileges' principles and controls to limit access to such individuals?
 - o Enforcement of standards for strong passwords, including minimum and maximum length of the password, and password composition?
- l) Have you developed and implemented privacy and security policies to inform the design of IT functionality and organizational business procedures?

Principle 3: Benefits to the Organization

- a) Avoids costly retro-fit of Applications to address privacy and security risks that are identified subsequent to implementation of the Application.

Principle 5: Full Life Cycle Protection—*PbD*, having been embedded into the Application prior to the collection of any PI, extends securely throughout the entire life cycle of the PI involved, from start to finish. Thus, *PbD* ensures *cradle to grave* protection of PI.

Principle 5: Full Life Cycle Protection

At each stage of the PI's life cycle, the following questions should be asked and remedial actions taken where risks, or gaps, are identified in your organization's security posture:

- a) Have you mapped the flows of PI from collection through use, disclosure, and destruction?
- b) Have you completed a data sensitivity analysis?
- c) Have physical and technical security risk assessments been conducted at every stage of a project?
- d) Have you identified all of the "touch and hand-off points" for PI for which security safeguards need to be applied?
- e) Have you assigned an 'accountable person' to be responsible for ensuring the mitigation of risks identified in your physical and technical security risk assessments?
- f) Have you implemented administrative, technical, and physical safeguards that are reasonable in the circumstances? Are these safeguards:
 - o Based on industry-accepted standards, frameworks, models, best practices, and guidelines for security, and in compliance with statutory requirements?
 - o Based on a defense-in-depth strategy to address identified threats and risks?
 - o Commensurate with the amount and sensitivity of the PI, and with the number and nature of those individuals with access to the PI?
- g) Do these administrative, technical, and physical safeguards ensure the secure retention, transfer, and destruction of PI?
- h) Have you ensured vendor and third party agreements clearly set out accountabilities and responsibilities for ensuring the implementation of safeguards and mandatory security controls?
- i) Does your organization require that assessments of security controls are conducted regularly throughout the life cycle of the PI to ensure its confidentiality, integrity, and availability?
- j) Have you established a retention schedule and procedures for the secure destruction of PI?
- k) Does the retention schedule:
 - o Clearly establish the length of time for which described categories of PI must be retained?
 - o Indicate the rationale for the retention of PI for these time periods?
 - o Require documentation describing the PI and the manner in which it may be stored according to the retention schedule?
- l) Do your destruction procedures:
 - o Require that PI must be destroyed in such a manner that it is not possible to recreate the information?
 - o Provide acceptable manners for destruction of PI in all formats in which it is held by the organization; e.g., electronic, paper?
 - o Remind individuals of the requirement to destroy PI that exists in electronic devices such as photocopier and facsimile machines before disposal of the device or its return to the supplier?
 - o Require that a certificate of destruction be prepared to include the nature of the PI, the date, identification of the individual who destroyed the PI, and the reason for the destruction of the PI at that time?

Information Technology	Accountable Business Processes	Physical Design & Networked Infrastructure
<p>a) Do you require vulnerability assessments and penetration tests to be conducted on an ongoing basis?</p> <p>b) Have you ensured that your information system audit logging functionality has the capacity to generate audit log alerts based on business rule thresholds and generate routine and ad hoc audit log reports?</p> <p>c) Do you monitor and report on system control and audit logs on an ongoing basis?</p>		

Principle 5: Benefits to the Organization

- a) Ensures security practices provide adequate protection of PI over its life cycle, including when it is accessed by, or in the physical custody of, a service provider.

Principle 6: Visibility and Transparency: *PbD* seeks to assure all stakeholders that whatever the Application involved, it is, in fact, operating according to stated promises and objectives. An organization's Applications must conform to its stated privacy and security practices. These practices are subject to independent verification, and are made visible and transparent to all.

Principle 6: Visibility and Transparency : Keep It Open

Accountability:

- a) Is the identity and contact information of the individual(s) responsible for privacy and security in your organization made available to the public and known within your organization?
- b) Have you implemented a policy that requires all 'public-facing' documents to be written in 'plain language' that is easily understood by the individuals whose information is the subject of the policies and procedures, and which includes information on how to assess the next level of address?
- c) Are the stated privacy and security practices of the Application subject to independent verification?

Openness:

- d) Do you make information about the policies and procedures and controls relating to the management of PI readily available to individuals?
- e) Do you publish summaries of all completed PIAs and TRAs?
- f) Do you publish summaries of independent third party audits of your information practices?
- g) Do you make available a list of data holdings of PI maintained by your organization?

Compliance:

- h) Have you implemented policies and procedures to receive, document, track, investigate, remediate, and respond to complaints? Have you developed a redress procedure?
- i) Have you implemented policies and procedures to receive, document, track, and respond to privacy inquiries?

Principle 6: Benefits to the Organization

- a) Ensures the public and other stakeholders are aware of your organization's privacy and security practices, and informs them of their privacy rights.
- b) Builds client trust.
- c) Builds reputation and may provide market advantage.

Principle 4 is the ultimate goal of the *PbD* philosophy.

Principle 4: Full-Functionality—Positive-Sum—Not Zero-Sum: *PbD* seeks to accommodate all legitimate interests and objectives in a positive-sum ‘win-win’ manner, avoiding unnecessary trade-offs. *PbD* avoids the pretence of false dichotomies, such as privacy vs. security. Privacy does not gain or lose at the expense of functionality and security.

Principle 4: Full Functionality - Positive-Sum - Not Zero-Sum

- a) For your Application, have you identified, documented, and made available throughout the organization:
 - All individuals’ interests related to the privacy, confidentiality, and security of their PI?
 - All business interests, drivers, and objectives?
 - Desired business functionality?
 - Privacy functionality requirements?
 - Security functionality requirements?
- b) Have you established structures and mechanisms whereby interested parties may enter into dialogue to ensure there are no trade-offs between functionality and privacy, and between privacy and security?
- c) Have you developed agreed-upon metrics and assessed whether all interests and objectives have been met?
- d) Do you reject privacy or security risk assessment recommendations that would result in trade-offs between functionality and privacy, and between privacy and security?
- e) Have you considered all risk mitigation recommendations against the intent of the *PbD* Principles to ensure consistency?
- f) Does the Application achieve all the interests and objectives sought to be achieved?

Principle 4: Benefits to the Organization

- a) If the other Principles are rigorously applied in the PIA analysis, the organization will develop an Application that not only satisfies the organization’s business objectives by providing the full functionality required to achieve these goals, but also an Application that protects the privacy of individuals with respect to their PI that is collected, used, and disclosed by the organization in its implementation of the Application.

6 Conclusion

The Framework describes an approach to the development of a *PbD PIA*. The *PbD* Principles are considered in the design of an organization's information technology, business process, physical space and networked infrastructure to ensure that a holistic approach to the PIA analysis is taken. The Framework ensures that the completed PIA captures:

1. The entire scope of an organization's privacy and data protection program; and
2. The design and functionality of information technologies, business processes, physical spaces and networked infrastructures.

As such, the Framework represents an important step in operationalizing the philosophy of *PbD* into a practical tool that organizations may use to incorporate *PbD* into organizational practices. Use of the Framework will guide organizations towards achieving a positive-sum outcome, and a win-win solution for both their customers and their businesses, by ensuring the protection of an individual's privacy without sacrificing functionality or security.

7 Sources

- *Access by Design: The 7 Fundamental Principles*, Dr. Ann Cavoukian, (www.privacybydesign.ca).
- *A Pragmatic Approach to Privacy Risk Optimization: Privacy by Design for Business Practices*, Nymity and Information & Privacy Commissioner Ontario (Nymity Inc. 2009).
- *Creation of a Global Privacy Standard*, Commissioner Ann Cavoukian, November 2006.
- *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study*, Ontario Information & Privacy Commissioner, February, 2011.
- *Smart Privacy*, Dr. Ann Cavoukian, August 13, 2009.
- *The 7 Foundational Principles* (www.privacybydesign.ca)
- *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers and Users*, Commissioner Ann Cavoukian, December 2010.