# *Privacy by ReDesign*:

## A Practical Framework for Implementation

November 2011

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner,
Ontario, Canada

Claudiu Popa, CIPP, CISA, PMP, CISSP
President and CEO,
Informatica Corporation
Founder, Informatica Research

# Table of Contents

Introduction ..... 1

Identifying Potential Targets for *Privacy by ReDesign* ..... 2

Framework for Implementing *Privacy by ReDesign* ..... 4

- Diagram: Implementing *Privacy by ReDesign* ..... 5
- Rethink ..... 6
- Redesign ..... 6
- Revive ..... 7

Laying the Foundations for Success ..... 7

- Building a Culture of Privacy: Strong Leadership and Goal-Setting ..... 7
- Protecting Privacy: Systematic and Verifiable Methods ..... 8
- Full Functionality: Achieving Win-Win Results ..... 8

The Road Ahead ..... 9

# Introduction

In May 2011, the Information and Privacy Commissioner of Ontario, Canada and Dr. Marilyn Prosch of Arizona State University introduced the concept of *Privacy by ReDesign* (*Pb$^R$D*), a framework for applying The 7 Foundational Principles of *Privacy by Design* to legacy and existing systems, including information technologies, business practices, and networked infrastructure.[1]

*Privacy by Design* has been steadily gaining momentum over the past several years as the new international standard in privacy and data protection. While its emphasis is on proactively embedding privacy at the outset, its principles also have relevance for existing and legacy systems.

*Privacy by ReDesign* is more than a retrofit – which is what often occurs when circumstances force organizations to focus on an immediate issue and apply a band-aid solution. *Pb$^R$D* is a transformative process. It is a framework for undertaking a proactive assessment of existing gaps in how personal information is used and managed, and addressing those gaps systematically. In this context, the principles of *PbD* are applied not as goals for a nascent system design, but rather as the end result of a successful *Pb$^R$D* initiative.

This paper builds on the ideas initially presented in the white paper, *Privacy by ReDesign*: Building a Better Legacy, and takes the next steps forward in exploring the application of *Pb$^R$D* in greater detail, laying out an implementation framework to assist executives in approaching *Privacy by ReDesign* projects effectively and identifying some critical success factors to support their efforts.

The guidance contained in this paper is intended to be relevant to leaders of organizations of all sizes, and all sectors – the transformative process will apply widely, regardless of the area involved.

1 Ann Cavoukian, Ph.D. and Marilyn Prosch, Ph.D., *Privacy by ReDesign: Building a Better Legacy*. (May 2011) http://privacybydesign.ca/content/uploads/2010/11/*PbRD*.pdf

# Identifying Potential Targets for *Privacy by ReDesign*

For any organization that wants to improve its privacy posture, the critical first step is to identify appropriate targets for potential remediation or transformation.[2]

Organizations may be prompted to consider *Pb^RD* projects for any number of reasons. In some cases, opportunities may arise as a result of a proactive strategy for improving the organization's privacy posture as part of existing management structures that support risk mitigation or brand/market positioning.

As noted in *Privacy by ReDesign: Building a Better Legacy,* organizations that have mature risk management or continuous improvement frameworks may already include consideration of legacy systems in those processes. Privacy requirements can and should be incorporated into these management frameworks, if they are not already. [3] This can support the identification of possible targets.

Likewise, organizations may wish to leverage a proven, standardized framework of controls such as COBIT, which enables clear policy development and good practice for IT control throughout organizations and emphasizes regulatory compliance, helping organizations to increase the value attained from IT. Such frameworks allow *PbRD* to be incorporated as a component of aligning with existing compliance requirements.[4] This type of approach makes it possible to leveraging existing audit processes and decentralize privacy assurance.

Opportunities to consider *Pb^RD* projects may also arise more reactively, for example as a result of:

- **External Factors:** such as changes in legal requirements or industry best practices, and new partnerships or outsourcing arrangements (including cloud computing).
- **Internal Factors:** such as ongoing risk management activities, technology upgrades, software modifications, changes in work processes or workflows, changes in the work force and/or expertise, and changes in accountability and governance.

2 A target is a legacy system, which consists of a collection of applications and processes, coordinated to perform a single or multiple functions, which represents the scope of a privacy remediation or enhancement project.

3 See, for example, Ontario Information and Privacy Commissioner, Ontario Lottery and Gaming Commission, and the YMCA: *Privacy Risk Management, Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default*. (April 2010) http://privacybydesign.ca/publications/accountable-business-practices/

4 COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

- **Competitive Forces:** such as the need to build consumer trust and loyalty, the threat of new market entrants, changes in both supply and consumer demand, and opportunities to seize competitive advantages.
- **Consumer Forces:** such as evolving user requirements, changes in customer expectations, and the diversity of customer expectations in various global markets.[5]

Organizational leaders may seize these windows of opportunity to improve privacy protection in existing functionality, or to implement new components to support responsible information management and render privacy the default condition, going forward. Such opportunities may also arise when a system developed for one purpose evolves to take on another, perhaps unintended use, with unexpected or poorly-understood consequences for privacy.

Where several potential targets for remediation have been identified, it may be necessary to perform an initial, high-level triage in order to prioritize projects. While many techniques can be used, a simple set of focused questions based on The 7 Foundational Principles of *Privacy by Design* may be quite effective. These will vary according to the size of the business or industry sector in which the organization participates.

### Sample Questions for Triaging PbRD Targets

- ☐ Does the target involve the collection, use, or disclosure of personal information? How sensitive is the personal information in question?
- ☐ Does the target collect more personal information than is absolutely necessary to fulfill the specified business purposes?
- ☐ Are users required to take specific actions to protect their privacy, or is privacy the default setting? Are user privacy preferences configurable?
- ☐ Could the introduction of additional privacy features constitute a competitive advantage for the organization?
- ☐ Does the target exhibit a potential compromise between functionality and privacy, such as offering conditional access to desirable features only to the detriment of privacy?
- ☐ Is personal information consistently protected throughout its entire lifecycle (i.e. collection, use, disclosure, retention, and disposal)?
- ☐ Are privacy policies effectively communicated to internal and external stakeholders?
- ☐ Is it clear to data subjects when and how personal information about them is being collected, used and/or disclosed?
- ☐ Has the target been designed and implemented to embrace the interests of users and data subjects (e.g. through strong privacy defaults, appropriate notice, and user-friendly options)?

5 Ibid., p 3.

Other useful techniques may include Privacy Impact Assessment methodologies 6 as well as the Generally Accepted Privacy Principles (GAPP) and Criteria.[7]

Regardless of how potential targets have been identified and whether an initial triage process has been completed, a more comprehensive review (for example, in the form of a full Privacy Impact Assessment) may be required on the part of the project team in order to establish the full scope of a *Pb^R^D* project.

## Framework for Implementing *Privacy by ReDesign*

In *Privacy by ReDesign: Building a Better Legacy*, we outlined the 3 R's of *Pb^R^D* : Rethink, Redesign, and Revive. These 3 R's may be used to anchor *Pb^R^D* projects, and to organize the phases of project work, as shown in the chart below. Note that the phases may, in practice, overlap, and that activities may occur in a different order than indicated here. Many of the activities will be iterative in nature.

This table focuses solely on the privacy aspects of target remediation or transformation. To the extent that transformation projects may open up opportunities to undertake other, non-privacy related enhancements, these must be reflected in a broader project framework that is beyond the scope of this current paper.

Just as *PbD* may be incorporated into any development methodology, *Pb^R^D* does not dictate a particular approach to transformation or remediation projects, and may be integrated into whatever approach an organization already uses for such projects. What is essential is that all interests and objectives, including privacy, be clearly documented, desired functions articulated, metrics agreed upon and applied, and trade-offs rejected as often being unnecessary, in favour of finding a solution that enables multi-functionality.

Importantly, even in scenarios where the target is an IT system or application, *Pb^R^D* cannot be viewed as just an IT project. Privacy expertise must be available and engaged through all phases of the workflow, and bring with it a multifaceted understanding of privacy issues and requirements, and an appreciation of consumer/client expectations. Depending on the nature of the project, there may be significant need for the competencies of functional experts, risk managers, change and process experts, and other specialists.

6 See, for example, Information and Privacy Commissioner/Ontario, *The Privacy Diagnostic Tool (PDT) Workbook* (Aug 2001), and *The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation* (Feb 2009), www.ipc.on.ca. See also the forthcoming *PbD* PIA, which will include a comprehensive assessment of the governance of, and accountability for, personal or personal health information collected, used, disclosed, retained and shared, as the case may be. www.privacybydesign.ca.

7 The Generally Accepted Privacy Principles (GAPP) were developed by AICPA and the Canadian Institute of Chartered Accountants (CICA). See http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx.

# Diagram: Implementing *Privacy by ReDesign*

Identify systems in need of transformation to target

Triage potential targets

| Phase | Rethink | Redesign | Revive |
|---|---|---|---|
| **Ojective** | Identify business and privacy requirements associated with the target system | Design and develop new controls to meet business and privacy requirements | Rollout redesigned, privacy-enhanced system |
| **Key Activities** | Confirm/establish business requirements<br><br>Evaluate existing system privacy controls against *PbD* Principles<br><br>Identify deficiencies<br><br>(gap analysis)<br><br>Define strategic business objectives, control requirements and initial implementation strategy | Design and build controls that meet business objectives while supporting *PbD* principles<br><br>Eliminate earlier existing non-compliant controls<br><br>Implement new controls<br><br>Test new controls | Revalidate the redesigned target system against *PbD* Principles<br><br>Deploy<br><br>Confirm successful integration of redesigned target system |
| **Outcome** | Clear project objectives developed | Redesigned target system with new privacy controls in place | Organizationally-integrated target system aligned with *PbD* Principles |

As shown in the diagram above, the task at the outset is to identify and triage systems in need of transformation or remediation to target. From there, the phases of project work may be mapped to the 3 R's – Rethink, Redesign, and Revive.

## Rethink

In the Rethink phase, the core objective is to identify the business and privacy requirements that are associated with the target system. This objective is achieved through a process that begins with establishing or confirming business requirements. A key component of this process is identifying the information requirements that align with the business requirements. Many organizations may find that they are collecting more information than is technically necessary to achieve their goals, thereby increasing their privacy risk.

The system's existing privacy controls must then be assessed against the requirements of *Privacy by Design*, with deficiencies being identified through a gap analysis. This will enable the strategic business objectives to be defined, and the resulting control requirements and initial implementation strategy to be developed.

By the end of this phase, clear project objectives will have been developed, marking the way forward.

## Redesign

In the Redesign phase, the core objective is to design and develop new controls that will align with both the business and privacy requirements identified in the Rethink phase. In some cases, best practices may be available to guide this work. In others, however, innovation and creative thinking will be required to develop positive-sum solutions that achieve full functionality – both privacy and business objectives.

The resulting new or improved controls must then be implemented and tested. The initial non-compliant controls must also be eliminated, once the new controls have been introduced.

By the end of this phase, a redesigned target system, with new privacy controls, will be in place.

## Revive

In the Revive phase, the core objective is to integrate the newly redesigned, privacy-enhanced system into the organization. Through this deployment, the real benefits of improved privacy practices will be realized. It is at this time that any issues related to how the improved system interacts with other systems in the organization will also arise and may be addressed.

At the end of the Revive phase, the organization will have achieved a fully-functional, integrated, privacy-enhanced system. Where necessary or appropriate, the process can then be repeated in the context of another target system, until all of the organization's legacy or existing systems have been remediated.

# Laying the Foundations for Success

Just as *Privacy by Design* fosters innovation by challenging system designers and engineers to think creatively and holistically about all of a system's requirements, *Privacy by ReDesign* similarly challenges organizational leaders to innovate, test, and discover what works best in their particular environment.

That said, experience has shown that the success of *Privacy by Design* projects is dependent, to a large extent, on strong leadership, taking a systematic approach, and consistent follow-through.

Similarly, while *Privacy by ReDesign* may be implemented in any of a number of ways, and linked with any of a number of existing processes within the organization, there are some factors that greatly increase the likelihood of success.

## Building a Culture of Privacy: Strong Leadership and Goal-Setting

Whether applied to information technologies, organizational practices, or networked information ecosystems, *Privacy by ReDesign* begins with an explicit recognition of the value and benefits of adopting strong privacy practices. This implies:

- A clear commitment, at the highest levels, to set and enforce high standards of privacy – higher than the minimal standards set out in most global laws and regulations.

- A privacy commitment that is demonstrably shared throughout, by user communities and other stakeholders, in a culture of continuous improvement.
- Established methods to assess the actual or potential privacy implications of designs, practices, and outcomes, and mitigate any privacy risks identified in proactive, systematic, and innovative ways.

Organizational leaders have a critical role to play in fostering a commitment to privacy at all levels of the organization. They must both foster and support a Culture of Privacy. Such a culture enables sustained collective action by providing people throughout the organization with a similarity of approach, outlook and priorities. It is what leads privacy to be woven into the fabric of day-to-day operations of the organization, at all levels.

## Protecting Privacy: Systematic and Verifiable Methods

Through the process of transforming or remediating technologies, operations, and/or information architectures, the development of privacy features should be approached in a holistic, integrative and creative way.

- Holistic, because additional, broader contexts must always be considered.
- Integrative, because all stakeholders and business interests should be consulted.
- Creative, because achieving privacy, at times, requires reinventing choices where existing alternatives may be unacceptable.

A systemic, principled approach to achieving privacy should be adopted – one that relies upon accepted standards and frameworks, which are amenable to external reviews and audits. All fair information practices should be applied with equal rigor, at every step of the exercise.

## Full Functionality: Achieving Win-Win Results

*Privacy by ReDesign* is not simply about declarations and commitments – it is about satisfying all of an organization's legitimate objectives, including privacy protection. The end goal is to achieve real, practical results and beneficial outcomes for multiple interests – a win/win strategy.

In order to achieve such a result, it is essential that all levels of the organization approach privacy with the right mindset. Leaders have a key role in setting the right

tone. Privacy must not be positioned as having to "compete" with other legitimate values, design objectives, and technical capabilities, in any given domain. Throughout the remediation or transformation process, full functionality must be supported, and, to the greatest extent possible, all requirements must be optimized in a complementary, not a conflicting, manner.

## The Road Ahead

While the full implementation of the principles of *Privacy by Design*, ideally at the outset of a new system, application, or process development, is the end state for which we strive, organizational and economic realities are such that practical, economically-sound approaches to implementing *PbD* in *existing* systems in the here-and-now are also essential.

Market leaders are increasingly building a body of experience and knowledge about the implementation of *Privacy by Design*. There is a clear need for practical guidance as to how to accomplish its objectives and implement its principles in existing systems.

As mentioned in *Privacy by ReDesign: Building a Better Legacy*, work is well underway in this area, including an initiative by Ernst & Young that looks at how to integrate the principles of *PbD* into IT transformation projects.

Fully implemented, however, *Privacy by ReDesign*, as an extension of *PbD*, is enterprise-wide in scope, encompassing all aspects of the corporate eco-system. This white paper is intended to serve as a resource for executives seeking to improve their organization's privacy posture, and provides a high-level overview of the implementation framework for successful $Pb^{R}D$ projects. We encourage further collaboration and development in this and related areas, including the development of detailed practical guidance for project staff and tools and resources to support project work. *Privacy by Design* will apply broadly in the future. *Privacy by ReDesign* allows the principles of *PbD* to apply *now* to existing and legacy systems. Why wait?

**Information and Privacy Commissioner of Ontario**
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

November 2011

Privacy by Design: www.privacybydesign.ca

Information and Privacy Commissioner,
Ontario, Canada