Privacy by ReDesign: Building a Better Legacy

www.privacybydesign.ca

May 2011

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

Marilyn Prosch, Ph.D., CIPP
Associate Professor,
W.P. Carey School of Business

Table of Contents

Privacy by Design: The Gold Standard

Privacy by Design (*PbD*), created by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, is a proactive approach to privacy protection that is preventative in nature. It seeks to avoid breaches and their attendant harm, instead of simply offering mechanisms for redress after the fact. It was originally conceptualized to circumvent the challenges that arise from treating privacy as an after-thought and attempting to "bolt it on" after the system has already been created.

PbD takes a holistic view of privacy protection, and prescribes that privacy be embedded directly into the design and operation of not only information technologies, but also of business practices, physical design and networked infrastructure. This broad-based perspective on privacy requires that attention be paid to responsible information management throughout all of the interacting, interrelated, and interdependent elements that comprise organizations and their assorted lines of business.

The objective of *Privacy by Design* – attaining the gold standard in the protection of personal information – may be achieved by practicing its 7 Foundational Principles:

The 7 Foundational Principles of *Privacy by Design*

1. **Proactive** not Reactive; **Preventative** not Remedial
2. Privacy as the **Default Setting**
3. Privacy **Embedded** Directly 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**

The concept of data minimization – the idea that the collection, use, disclosure and retention of personal information should be minimized wherever, and to the fullest extent, possible – underlies all of these principles.

Many systems in existence today were designed just as data storage became cheaper, and reflect both this fact and a "more is better" philosophy. Such systems need to be updated to reflect the paradigm shift from data hoarding to data minimization. When organizations refrain from collecting unnecessary data, they minimize privacy risks and reduce their burden of care. They may also reduce the costs of data protection. The principle of data minimization helps to ensure that privacy becomes the default condition throughout the system – the hallmark of an effective *PbD* implementation.

The Tipping Point

After years of research and advocacy, *PbD* is now being widely adopted by a growing number of organizations. Around the world, there is mounting momentum behind enshrining The 7 Foundational Principles of *PbD* into privacy policies and regulatory frameworks. *PbD* was endorsed, for example, in the U.S. Federal Trade Commission's 2010 paper, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policy Makers*, as well as in the European Commission's recent consultation paper.

Last year, Data Protection and Privacy Commissioners from around the world met in Jerusalem and unanimously adopted a *PbD Resolution* that, among other things, encourages regulators to incorporate the principles of *PbD* into law within their respective jurisdictions. We can expect to see much more of this type of activity around the world, in the coming years. *PbD* has truly become an international standard.

Complementing this well-established support for the concept of embedding privacy into systems right from the outset, is the growth of *PbD* as a *practice* that is being embraced by leading organizations that are developing cutting-edge applications. Significant projects in nascent areas such as the Smart Grid, Biometric Facial Recognition, IP-geolocation, and a variety of mobile applications demonstrate innovative applications of the principles of *Privacy by Design* – and pave the way for future development.

Privacy by ReDesign: A Transformative Process

There is no longer any question that tackling privacy issues upfront, and embedding privacy protections directly into new systems, processes, and architectures, is optimal from both a privacy and a business perspective. Indeed, most businesses are no longer asking, "why should we do this?" but rather, "how do we do it?"

The reality, however, is that it is not always possible to embed privacy directly from the outset. Most organizations operate in the context of existing, relatively mature IT systems and businesses practices, which they have developed and evolved over time, as business or other needs have dictated. Replacing such systems, particularly if they generally continue to meet the organization's primary business needs, is often not on the agenda.

Does this mean that The 7 Foundational Principles of *Privacy by Design* have no relevance in organizations with longstanding systems, including legacy systems, and well-established business processes? No! What it means is that we need to transform existing legacy systems into positive-sum, privacy-embedded systems.

Privacy by Design presents a clear and effective strategy for meeting the objective of attaining the highest degree of privacy protection possible. It benefits individuals, providing them with important assurances about how their personal information is being managed. But it is also benefits businesses, which may enjoy sustained competitive advantages from the trust that responsible privacy practices engender with their customers.

For the same reasons, *PbD* is equally relevant to established systems as it does for nascent ones. Previously developed and implemented systems, however, cannot engage with *Privacy by Design* in the same manner as nascent ones. Instead, the task must be approached as one of *Privacy by ReDesign* (*Pb^{R}D*) – an extension of *PbD*.

Privacy by ReDesign is a new approach to applying the 7 Foundational Principles of *Privacy by Design* to existing systems: information technologies, business practices, physical design, and networked infrastructure. Clearly, since existing systems are already operational and pervasive throughout organizations, the principles cannot be embedded *from the outset*. Instead, the objective must be to approach the end state of *PbD* – the highest standard of privacy protection – by seizing opportunities to Rethink, Redesign, and Revive these systems.

The 3 R's of *PbRD*: Rethink, Redesign, and Revive

Business systems are organic. Their components, including information technologies, business practices, physical design, and networked infrastructure, evolve as a result of any of a number of factors, which may be generally grouped under the following categories:

- **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 work flows, changes in the work force and/or expertise, and changes in accountability and governance.
- **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.

These forces may open windows of opportunity to either implement or improve privacy protection in existing aspects of the system, or to make choices about new system components that support responsible information management practices and render privacy the default condition. These are opportunities to Rethink, Redesign, and Revive aspects of the system, in whole or in part, based on the 7 Foundational Principles of *Privacy by Design*.

- **Rethinking** invites organizations to review their risk mitigation strategies, existing systems, and processes – including information technologies, business practices, physical design, and networked infrastructure – and consider alternative approaches that are more privacy-protective. This may include revisiting assumptions about how much personal information is necessary for the system to operate, and how long it needs to be retained in identifiable form.
- **Redesigning** represents the opportunity to enable or implement improvements in how the system functions from a privacy perspective, while also ensuring that it continues to achieve key business requirements in a doubly-enabling positive-sum, win/win relationship. Redesigning may likely require that less data be collected, and these changes may need to be cascaded back to stored databases where possible, to delete these unnecessary fields of data.
- **Reviving** the system in a new, privacy-protective way is the ultimate goal!

Just as *PbD* challenges organizations to think creatively about how all system objectives – including privacy – can be met from the outset, *Pb^{R}D* challenges them to identify and act on opportunities to improve privacy practices going forward by redesigning components of existing systems, based on where they are today.

Where new system components are being added to existing systems, they can be designed with privacy embedded from the outset, in what basically amounts to a contained implementation of *Privacy by Design*. Existing systems and processes, by contrast, may need to be wholly redesigned to reflect privacy objectives. The re-engineering process may be undertaken as a single project or, perhaps more likely, be rolled out incrementally, taking advantage of an initial privacy gap analysis or Privacy Impact Assessment as a roadmap, and seizing opportunities to make small, cumulative adjustments as they arise through natural and/or planned system evolution.

Rethinking, Redesigning, and Reviving existing systems and their components can involve measures that range from the simple to the complex, and may include policy, operational, technology, or management changes. Changes such as revisiting database permissions, for example, or enabling access logging features, can make a profound difference in the extent to which personal information is accessed and used within an organization, improving both privacy and security. Similarly, a review of data retention policies can result in the secure destruction of records that no longer serve a business purpose, reducing the organization's burden of care and enhancing privacy.

Next Steps: Future Research Directions

Mature organizations often have frameworks in place, such as risk management or continuous improvement programs, which may include legacy systems in their purview. If they are not already, privacy requirements should be incorporated into these management frameworks and, ultimately, reflected in existing systems. With *Privacy by Design* being widely recognized as the new gold standard for the protection of personal information, there is a clear need for practical guidance as to how to accomplish its objectives and implement its principles in this environment.

Some work in this area is already taking place. Ernst & Young has been looking at the technological aspects of this issue, mapping common challenges and developing a methodology for integrating the principles of *PbD* into IT transformation projects.[1] Further work is needed in this area, as well as in other system areas such as business practices, physical design, and networked infrastructure. Fully implemented, *Privacy by ReDesign*, as an extension of *PbD*, is system-wide in its application, encompassing all aspects of the corporate eco-system.

The Information and Privacy Commissioner of Ontario, and Arizona State University's *Privacy by Design* Research Lab, are promoting research in this area and intend to drive the development of practical tools that support meaningful implementation of privacy in legacy systems, including those that leverage existing management processes by extending them to include privacy considerations. We look forward to the participation of industry leaders and experts in the development of tools and resources such as Privacy Impact Assessments, Risk Management Frameworks, IT Security tools, Privacy Maturity Models, Project Management instruments, best practices, and success stories.

While the full implementation of the principles of *Privacy by Design*, ideally at the outset, is the end state for which we strive, we must not let perfection stand in the way of progress. Indeed, in some situations, progress may be the only path available, and must be actively embraced. Organizational and economic realities are such that practical, economically-sound approaches to implementing *PbD* – the gold standard in privacy – are essential, for both nascent and existing systems.

[1] The results of this work will be presented in November 2011 at the 33rd Annual Conference of International Data Protection & Privacy Commissioners in Mexico.

PbD

www.privacybydesign.ca

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

May 2011

http://www.privacybydesign.ca

Information and Privacy Commissioner,
Ontario, Canada