NYMITY
Toronto/NYC/London

A
Pragmatic Approach
to
Privacy Risk Optimization

Privacy by Design for Business Practices

This paper introduces Nymity's Privacy Risk Optimization Process (PROP), a process that enables the implementation of privacy into operational policies and procedures, which embodies in Privacy by Design for business practices.

Nymity Inc.

Canada:

Brookfield Place
161 Bay Street
26th Floor
Toronto, Ontario
M5J 2S1

United States:

245 Park Avenue
39th Floor
New York City, NY
10167

Europe:

Berkeley Square House
2nd Floor
Berkeley Square
London, England
W1J 6BD

www.nymity.com

Information and Privacy Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

www.privacybydesign.ca

NYMITY
Toronto, NYC, London

This paper was produced by Nymity and the Office of the Information and Privacy Commissioner of Ontario, Canada. It will be presented by Terry McQuay, President of Nymity, at "Privacy by Design: The Definitive Workshop," in Madrid, Spain, on November 2nd, 2009. The workshop will be hosted by Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada, and Yoram Hacohen, Head of the Israeli Law, Information and Technology Authority.

Copyright 2009 by Nymity Inc.

All rights reserved. This document may be reproduced and distributed as part of professional services or within the context of professional practice, provided that reproduced materials are not in any way directly offered for sale or profit. For information about the procedure for requesting permission to make copies of any part of this work, please visit www.copyright.com or call (978) 750-8400.

NYMITY
Toronto, NYC, London

Table of Contents

© Nymity Inc. 2009

Executive Summary

Background

In 2004, Nymity, a global privacy and data protection research firm, recognized that traditional approaches to implementing privacy often placed constraints on organizations' business practices. Nymity initiated a research project with the objective of creating an approach to privacy compliance which would enable business to prosper while advancing privacy. Multiple approaches were developed and tested[1] and ultimately, a process was developed which enabled organizations to effectively build privacy into their business practices.

Aware of how Nymity's research helped organizations build privacy into business practices, Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, asked Nymity to make the process publicly available and to present it at the first, "Privacy by Design: The Definitive Workshop," in Madrid, Spain, on November 2nd, 2009.

This jointly developed paper introduces Nymity's Privacy Risk Optimization Process (PROP), a process that enables the implementation of privacy into operational policies and procedures, which results in Privacy by Design for business practices.

Risk Optimization

The PROP is based on the International Organization for Standardization (ISO) concept that risk can be both positive and negative. Based on this concept, ISO also defines Risk Optimization[2] as a process whereby organizations strive to maximize positive risks and mitigate negative ones. The PROP uses these concepts to implement privacy into operational policies and procedures.

To do so, the PROP targets policies and procedures of business activities that involve or affect the collection, use, storage, destruction or disclosure of customer and employee personal data. For these business activities, the PROP provides:

- Opportunities – Favourable conditions or situations that can enhance business practices by introducing privacy controls; and
- Positive Privacy Controls – Enabling privacy while enhancing business practices (win/win).

Introduction to Privacy by Design

Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, developed the concept of "Privacy by Design" in the '90s. Privacy by Design or PbD, as it has come to be known, asserts that privacy protection should be embedded in an organization's technology, business practices and physical design. Embracing a positive-sum (win/win), as opposed to a zero-sum (win/lose), approach, organizations offer default privacy protection without compromising security, performance or functionality—enabling multiple goals to be achieved. PbD ensures that individuals retain control over their personal information and that organizations gain a sustainable competitive advantage—good privacy is good business.

[1] Nymity's risk optimization research was initiated in 2004 and evolved into the creation of risk and controls checklists that are used by hundreds of organizations to assist them with privacy management.
[2] ISO/IEC GUIDE 73:2002 (3.4.3)

© Nymity Inc. 2009

4 Steps of the PROP

The PROP works for small projects or large, complex projects. It scales based on the amount of resources allocated and the organization's needs. The PROP does not require a great deal of training, questionnaires, detailed spreadsheets, software, extensive work plans or a large team of experts. The PROP provides a pragmatic and effective approach for implementing corporate privacy policies through business practices.

The four steps of the PROP are:

1. Create a Project Plan;
2. Create Risk and Positive Control Checklists;
3. Create a Risk Optimization Plan; and
4. Implement the Risk Optimization Plan.

The process is applied to specific business activities in which there is a privacy concern, or where there are opportunities to use privacy to gain business advantage.

Compliance

For some organizations, compliance with laws and regulations is the primary motivator to invest in privacy and the PROP is particularly well-suited to help develop or enhance operational policies and procedures to achieve compliance. The challenge with traditional approaches to compliance is that they are generally resource-intensive and the results tend to constrain business. The PROP allows for resources to be allocated tactically and as it focuses on opportunities and positive privacy controls, the results enable business rather than constrain business.

Learn from Common and Leading Practices

There is a wealth of information and expertise available that supports privacy management and the PROP allows organizations to exploit that information. Organizations no longer have to work in a vacuum or wonder how other organizations address a similar situation. The PROP includes a research phase in which the project team learns common and leading practices from other organizations that have faced similar problems, gaining creative approaches to compliance. The research phase can be global in nature and allows organizations to learn from expertise around the world.

Privacy by Design

The use of the PROP enables organizations to use the guiding principles of Privacy by Design in their privacy management and compliance initiatives. Thus, the PROP provides a concrete "how to" for implementing Privacy by Design into business practices.

Many of the concepts outlined in this paper are already used by organizations with mature privacy management programs. Organizations with limited resources to invest in privacy will most likely find considerable value in following the PROP.

© Nymity Inc. 2009

Section 1: Prevailing Privacy Management Myths

Historically, multiple myths have surrounded privacy and data protection within the business context which have served to discourage organizations from taking more than minimal strides to integrate privacy controls into their core business practices. Here are just a few of these false beliefs:

"Privacy constrains business operations"

Many organizations believe that implementing privacy controls into their business practices will constrain their business operations. For example, they believe that privacy controls will inhibit sales, marketing, customer service, telemarketing, social networking, and product development. Some believe that privacy controls will cause an operational nightmare because of restrictions on outsourcing, records management programs, security, access controls and cross-border/international data transfers. With respect to their employees, some organizations maintain that privacy controls preclude using employee-monitoring technology, or conducting incident-based investigations, drug and alcohol testing, whistleblower programs and background checks.

"Privacy is nothing more than compliance"

For many organizations, the impetus for implementing privacy programs has been the emergence of laws and regulations that create rules about managing personal data. Some treat the word *privacy* as synonymous with *compliance,* and as such, privacy has become a legal issue, dealt with by Legal and Compliance departments. Prior to the introduction of laws, privacy—if dealt with at all—was a business issue, focused on customers and employees, and dealt with by Marketing and Human Resources departments. Historically, organizations that valued privacy treated it as a respect issue: it was about confidentiality, with a focus on the responsible uses of personal data. But now, most organizations treat privacy as a matter of legal compliance.

"Implementing privacy controls will be expensive"

Without any ability to realize a measurable business gain, some organizations believe that investments in privacy management are expensive, so instead, use a *risk management* approach to avoid potential future costs that could arise from non-compliance. But this approach is difficult to evaluate. Often, organizations resist investments due to their unsubstantiated belief that privacy is

Privacy by Design

One of the key principles of PbD is that it addresses what Dr. Cavoukian describes as the prevailing zero-sum mentality whereby privacy is pitted against efficient business practices – an inherently false dichotomy. PbD is the opposite - a positive-sum model which eliminates the dichotomy by ensuring that privacy has a positive impact on business practices and ultimately, therefore, on business operations.

A zero-sum paradigm describes a concept or situation in which one party's gains are balanced by another party's losses—win/lose. In a zero-sum paradigm, implementing privacy controls for business practices (e.g. to comply with privacy laws) is viewed as an obstacle in achieving overall business objectives.

Conversely, the positive-sum paradigm demonstrates that the implementation of positive privacy controls and opportunities for business practices results in a mutually beneficial gain—win/win. Adopting a positive-sum approach allows the organization to increase user privacy and achieve gains in business results.

© Nymity Inc. 2009

expensive and offers no business benefits like cost savings, time savings, or increase in revenue.

Section 2: Understanding the Components of the Privacy Risk Optimization Process (PROP)

To apply the PROP, it is important to understand its components. Although the PROP is easy to use, it is critical to understand the concepts of risk optimization to use it effectively.

Risk Optimization

The PROP is based on International Organization for Standardization (ISO) standards. One of the major advantages of ISO's approach to risk management is that the standards include both the positive and negative aspects of uncertainty (otherwise known as "risks"). ISO Guide 73[3], which defines much of the vocabulary for the PROP, deals with risk management from both the positive and negative perspectives. This allows opportunities to be realized while threats are averted or minimized, and vulnerabilities are addressed. ISO envisioned organizations wanting to focus on Risk Optimization,[4] *"a process, related to a risk, to minimize the negative and to maximize the positive consequences and their respective probabilities."* Risk Optimization is the core of this methodology.

Using an international standard for definitions and concepts for risk ensures the PROP is globally relevant and allows it to work in conjunction with other risk and privacy management methodologies.

Risk Optimization versus Risk Management

In some cases, risk optimization is a more efficient approach to privacy management than traditional approaches that are based on pure risk management structures. Risk Management[5] is defined as "'*coordinated activities to direct and control an organization with regard to 'risk.*" Although the objective may be similar, risk optimization has two major advantages over risk management. Risk optimization is:

1. Efficient, as there are fewer steps, and no requirement for questionnaires, complicated spreadsheets, or software. It does not require a great deal of training and there is no need to become an expert on risk management.

2. Opportunistic, as it enables organizations to uncover areas where operations can be enhanced.

PROP versus a Privacy Impact Assessment

The PROP is not a replacement for privacy impact assessments (PIAs) or any methodology that audits or assesses privacy. The PROP is better suited for the implementation phase of a compliance program and is not appropriate for assessing compliance. The PROP does not include questionnaires or criteria in which to conduct an assessment and it should not be used for such purposes.

When an organization conducting a privacy audit or a PIA identifies the need to update or create an operational policy or procedure, the PROP is a pragmatic approach to achieving that objective. The PROP can also be useful when research is required for complicated PIAs.

[3] ISO/IEC Guide 73:2002 Risk management - Vocabulary - Guidelines for use in standards
[4] ISO/IEC GUIDE 73:2002 (3.4.3)
[5] ISO/IEC Guide 73:2002

© Nymity Inc. 2009

In cases where a traditional approach to privacy management is more appropriate, the PROP can be used with the traditional approach as it can assist in conducting gap assessment and creating more positive mitigation strategies.

Business Activities

Privacy Principles[6] (commonly referred to as Fair Information Practices) work well for creating corporate-wide privacy policies and providing a top-down governance structure for creating a corporate privacy management program. The challenge with Privacy Principles is that they can be too high-level to effectively provide guidance to business practices.

The PROP does not follow a principle-based approach, but rather elects to focus on categories of business practices called "Business Activities." A Business Activity is defined as:

> "A *process that involves or affects the collection, use, storage, destruction, or disclosure of customer and employee personal data.*"

Examples of processes that "involve" the collection, use, storage, destruction, or disclosure of customer and employee personal data include background checks, cross-border transfers, discovery, investigation, online behavioral advertising, data-sharing with affiliates, telemarketing, use of Social Security Numbers, vendor management and tele-commuting.

Examples of processes that "affect" the collection, use, storage, destruction or disclosure of customer and employee personal data include breach response, personal data definition, privacy audits, notice provision, registration and notification, and employee training.

PROP and Privacy Principles?

The PROP does not compete with a Privacy Principle approach to privacy management; it simply works at a different level. In fact, PROP is typically used to implement operational policies and procedures that are based on Privacy Principles' corporate privacy policies.

Structuring the PROP on Business Activities allows for the development or updating of policies and procedures to be focused on a single business activity or a collection of business activities that make up a business operation. An organization can select one or more business activities based on the resources available and organizational priorities. This level of granularity allows organizations to focus on specific problems or opportunities in important operational areas and deploy limited privacy management resources to achieve maximum returns.

The Figure 1 provides examples of common European business activities that involve and affect the collection, use, storage, destruction, or disclosure of customer and employee personal data.

[6] Privacy Principles are based on many sources, including the following: OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; the AICPA/CICA Generally Accepted Privacy Principles (GAPP); APEC Privacy Framework; Canadian Standards Association Q830-03-CAN/CSA Model Code for the Protection of Personal Information

© Nymity Inc. 2009

Figure 1. Example of European Business Activities[7]

Legal	Customer	Employee	Operational	Data Transfers
Involve □ Lawful Disclosures □ Discovery Affect □ Breach Response □ Defining Data Controller □ Defining Data Processor □ Defining Personal Data □ Defining Data Processing □ Defining Equipment /Establishment □ Appointing Representatives □ Appointing Data Protection Officer □ Registration and Notification □ Establishing Legal Grounds for Processing □ Understanding Enforcement Actions	Involve □ Email Marketing □ Direct Marketing □ Telemarketing □ Use of Warning Markers □ Conducting Credit Checks □ Online Behavioural Advertising □ Online Communities and Collaboration □ Customer Privacy Policy/Notice □ Customer Authentication Affect □ Privacy notice	Involve □ Whistleblowing Hotlines □ Employee Investigations □ Conducting Background Checks □ Drug and Alcohol Testing □ Working with Work Councils □ Employee Authentication □ Employee Monitoring Affect □ Employee Privacy Policies □ Obtaining Employee Consent	Involve □ Handling Access Requests Affect □ Application Development □ Developing a Compliance Strategy □ De-Identifying Personal Data □ Information Security – Organisational Measures □ Information Security – Technical Measures □ Information Security – Physical Measures □ Data Destruction □ Data Retention □ Use of Encryption □ Use of Cloud Computing □ Use of Cookies □ Use of CCTV in Public Places □ Privacy Audits □ Privacy Impact Assessments □ Use of Tracking/Location Devices	Involve □ Outsourcing □ Mergers and Acquisitions Affect □ Selecting a Data Transfer Mechanism □ Using a Data Transfer Mechanism – Consent □ Using a Data Transfer Mechanism – Safe Harbor □ Using a Data Transfer Mechanism – Binding Corporate Rules □ Using a Data Transfer Mechanism – Standard Contract Clauses □ Using a Data Transfer Mechanism – Exemptions □ Onward Transfers □ Selecting a Dispute and Enforcement Mechanism

Example: USA - Customer Authentication

The business activity "Customer Authentication" will be used as an example throughout this paper. Customer Authentication[8] is defined as "*the process of verifying the identity of a person or entity*." In general, organizations authenticate customers prior to permitting them to access systems or computer applications, or prior to providing personally identifiable information in person or on the telephone. Authentication is distinct from authorization as authentication confirms the identity of the individual but does not address access rights.

Privacy Risk

Risk[9] is a "*combination of probability of an event and its consequence*." Business Activities that involve or affect the collection, use, storage, destruction, or disclosure of customer and employee personal data present privacy risks. The PROP divides privacy risk into threats, vulnerabilities, and opportunities.

[7] Nymity's PrivaWorks
[8] Federal Financial Institutions Examination Council.
[9] ISO/IEC Guide 73:2002

© Nymity Inc. 2009

Threats	Vulnerabilities	Opportunities
Threats[10] are any potential situation (or event) that can have a negative impact on the organization.	Vulnerabilities[11] include any attribute of a business activity that could be exploited by or through one of the threats resulting in a negative event.	Opportunities are favourable conditions or situations where business practices are enhanced by introducing privacy controls.

Example: For the business activity of "Customer Authentication," the following are examples of potential threats, vulnerabilities, and opportunities.

Threats:

- criminal pretexting an organization resulting in harm to customers or employees
- failing to authenticate the legitimacy of businesses or individual before disclosing personal information causing harm or embarrassment to the individuals affected
- disclosing information to a family member without the consent of the individual about whom the personal data relates to
- customer dissatisfaction due to the requirement for obscure, excessive or inappropriate personal information
- employee or system failure to properly authenticate prior to access to financial accounts resulting in financial loss to customer and/or company

Vulnerabilities:

- collecting driver licenses, for example to be used for fraud prevention
- using a government identifier such as a social security number
- not effectively verifying the age or identity of website users
- verifying customer's identity through information pulled from a public database
- use of single-factor authentication for high-risk transactions
- allowing short character length for password requirements
- use of keychain payment cards that can be stolen
- password recovery process less rigorous than the initial registration
- not checking for re-identification of anonymized information published to the web

Opportunities:

- reducing time and cost by implementing electronic voice authentication
- eliminating fraud by using driver's licenses hashing technique to eliminate the use of personal information
- ensure authentication by implementing a call back process
- increase customer satisfaction by:
  - streamlining call center processes
  - increased training of returns desk employees
  - teaching customers about phishing and identity theft
- reducing the changes of a data breach and the resulting breach notification requirements by implementing physical security for paper collections

[10] ISO/IEC 13335-1:2005 defines threat as "a potential cause of an unwanted incident, which may result in harm to a system or organization." Threats are consider the cause of a situation. Risk management methodologies include an attempt to quantify a probability of occurrence. Typically this is done with an ARO (annualized rate of occurrence).
[11] ISO/IEC 13335-1:2005 defines vulnerability as "a weakness of an asset or group of assets that can be exploited by one or more threats."

© Nymity Inc. 2009

Threats and Vulnerabilities = Negative Risk

Threats and vulnerabilities are typically thought to be risks as they represent the possibility of a negative consequence of an event. Minimizing threats and vulnerabilities is ultimately the primary motivator for any privacy management exercise, and the PROP helps organizations minimize these negative risks through the effective development of operational policies and procedures.

Opportunities = Positive Risk

ISO definitions of risk allows for the somewhat foreign concept of *positive risk*. To most, positive risk sounds like an oxymoron, but it is the foundation of risk optimization and thus a critical concept in the PROP. As shown below, positive risk helps organizations by identifying and implementing opportunities to enhance business practices.

In practice, the PROP focuses on opportunities that help organizations discover better ways of addressing the negative risk—opportunities that mitigate the threats and vulnerabilities without constraining business.

The PROP help organizations meet PbD Principle 4:

Full Functionality — Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is indeed possible to have both.

Privacy Controls

A *Control*[12] is a "*means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management , or legal nature.*" Privacy risk is mitigated by implementing privacy controls for Business Activities that involve the collection, use, storage, destruction or disclosure of customer and employee personal data.

Negative Privacy Controls

Controls that enable privacy but constrain business (win/lose) are negative privacy controls. The PROP strives to minimize the use of negative privacy controls by focusing on positive privacy controls. An example of a negative privacy control would be an overly rigorous verification process where the use of information provided by an applicant is matched against information available from trusted third party sources such as a credit report.

Positive Privacy Controls

Positive privacy controls enable privacy and business practices (win/win).

Positive privacy controls are implemented to minimize or eliminate threats and vulnerabilities and to take advantage of opportunities.

[12] ISO/IEC 17799:2005

© Nymity Inc. 2009

In practice, one of the main advantages of the PROP is the focus on opportunities. It has been found that, in many cases, the opportunities themselves are a good source for positive privacy controls.

The only challenge with positive privacy controls is that they may not be obvious. The negative controls are easier to identify than positive controls. The PROP requires the use of positive privacy controls.

For a partial example of positive privacy controls for the business activity "Customer Authentication," see Appendix C.

Privacy Management Business Activities are Privacy Controls

The PROP recognizes privacy management activities as both a business activity and a privacy control. For example, privacy audits, creating a privacy notice, employee awareness and training are both business activities and privacy controls. The granular design of PROP is particularly well suited in helping organizations create and implement privacy management business activities as the PROP provides the specific details that are required.

Compliance

For some organizations, the main motivator for investing in privacy is compliance. For these organizations, the PROP helps them implement or update their operational policies and procedures to comply with privacy and data protection laws. The PROP also assists organizations in complying with codes and standards and implementing corporate policies and governance structures into business practices.

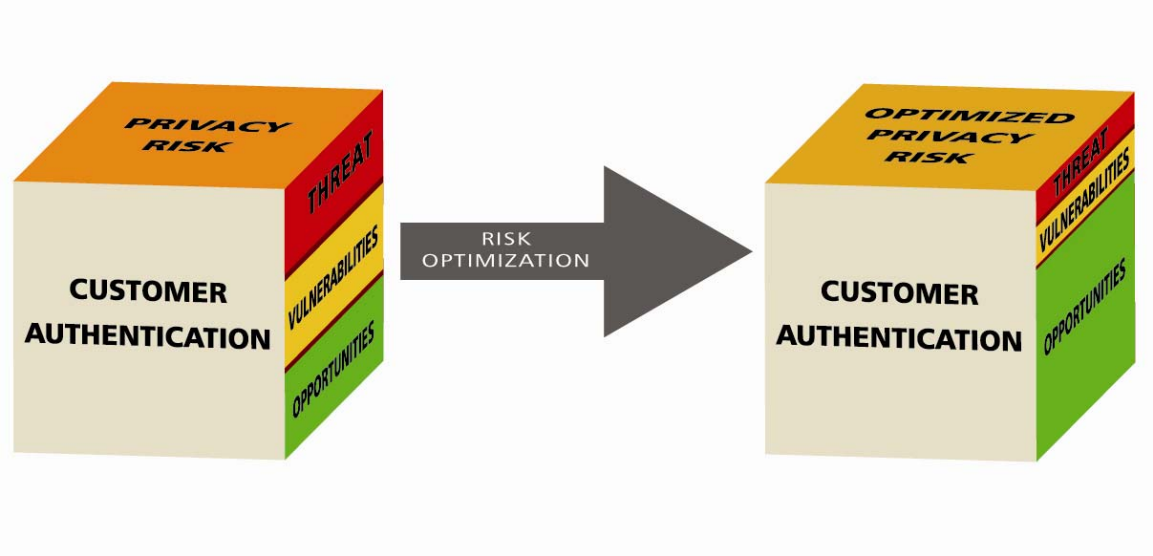
To apply the PROP for the purpose of compliance it is best to consider compliance risk as:

Compliance Threats	Compliance Vulnerabilities	Compliance Opportunity
A compliance threat is an event that would lead to being found non-compliant. For example a customer complaint leading to an investigation from a regulator or attorney general.	Compliance vulnerabilities are attributes of a business activity that are non-compliant. For example, the collection of a driver's license during a return of a product as a means to authentication and fraud prevention would find an organization non-compliant in some jurisdictions.	Compliance opportunities are situations where the organization can take advantage of becoming or being compliant, for example a competitive differentiator. For example, a 3rd-party locating a customer service call center in a specific jurisdiction to create a competitive differentiator to target customers concerned about cross-border transfers of personal customer data.

One of the challenges with traditional approaches to compliance is that some organizations treat the process as "good enough to pass" exercise. This approach often does not help get to the heart of the goal of better privacy, misses opportunities to improve business practices, restricts business practices and builds resistance for privacy in the business units. The advantage for using the PROP as part of the organization compliance program is that it enables the organization to easily go beyond the minimum generic compliance requirements.

© Nymity Inc. 2009

Section 3: Application of the PbD Risk Optimization Methodology



The four steps of the PROP are:

1. Create a Project Plan
2. Create Risk and Positive Control Checklists
3. Create a Risk Optimization Plan
4. Implement the Risk Optimization Plan

Before reviewing the PROP's four steps, it is important to reiterate the need to focus on Business Activities. Some projects will focus on a specific Business Activity, such as "Customer Authentication." For example, an organization was concerned about the results of a regulatory action against one of their competitors which required the competitor to make significant changes to their customer authentication process. The organization decided this was a significant concern and initiated a project to review their customer authentication process. The project was easily justified as the new regulatory expectations could have resulted in more authentication steps thus causing longer call times. Longer call times increase costs and past experiences have shown the longer it takes to authenticate the customer's identity, the more frustrated the customer becomes and overall customer satisfaction decreases.

Some projects may involve multiple Business Activities. For example, a new Records Management policy was created and the human resources department wants to use the PROP to update the procedures related to records management. In this case, the Business Activities of "Records Retention," "Records Destruction," and "Safeguarding Data" were chosen to be the focus of the project.

© Nymity Inc. 2009

Step 1: Create a Project Plan

For the specific area of concern, the first step is the creation a project plan. The project plan establishes the scope of the project which includes the objective, the Business Activity or Activities, participants and resources. One of the advantages of the PROP is that there are definitive steps to which time can be allocated reducing the likelihood of the project going beyond the original intentions and requiring more time and resources.

The first component in this step is to identify the appropriate Business Activity or Activities. This may seem simple but the organization must avoid selecting a business function instead of a Business Activity. For example, "call centre" would not qualify as a Business Activity as it does not meet the definition: *"A process that involves or affects the collection, use, storage, destruction or disclosure of customer and employee personal data."* A call center is a function involving a set of Business Activities including "Customer Authentication," "Call Recording," and "Telemarketing" among others.

The PROP project plan includes, but is not limited to:

- Objective
- Background
- Project Team and Stakeholders
- Business Activity/Activities
- Applicable Laws and Regulations
- Participants
- Resources
- Research Time
- Research Strategy

Research Strategy

A research strategy is a plan the project team develops to create risk and positive controls checklists. It's a critical component of the process, and is outlined in more detail in Step 2.

The PROP help organizations meet PbD Principle 1:

Proactive not Reactive; Preventative not Remedial

The Privacy by Design (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 them from occurring. In short, Privacy by Design comes before-the-fact, not after.

Step 2: Create Risk and Positive Control Checklists

There is a wealth of privacy information and expertise available that can help organizations with privacy management, and the PROP enables organizations to exploit that knowledge. Based on research and education, organizations can create a risk checklist and a positive control checklist for the selected Business Activities. Creating these checklists is critical for the success of the PROP as it is the foundation for creating the Risk Optimization Plan for each of the Business Activities. Between 50% and 75% of the time allocated to the project should be invested in this research phase.

© Nymity Inc. 2009

Not only does this phase prepare for creating the Risk Optimization Plan, it provides in-depth privacy education, identifies relevant opportunities, and ultimately identifies pragmatic, positive privacy controls. The PROP is scalable as the resources are deployed based on the project plan. The participants use the research strategy (described below) from the plan and create the risks checklist and a positive controls checklist for each of the Business Activities based on the time allocated.

Risk Checklist

The Risk Checklist is a list of known threats, vulnerabilities, and opportunities for the Business Activity. When creating the risk checklist, it is not necessary to delineate between threats, vulnerabilities, and opportunities. In fact, the differences may simply be the context in which they are presented. An example of a "Customer Authentication" vulnerability is not having a call-back process to ensure a customer's identity. Or it could be positioned as an opportunity to demonstrate customer confidentiality and enhance customer service by implementing a call-back program. Another example: not using 2-factor authentication for applications requiring a higher level of security, such as access to online financial accounts. It could be positioned as an opportunity by demonstrating to customers that the organization has effective security controls to protect their personal information, thereby increasing customer confidence and building trust. Risk checklists should be newly created for every project.

Positive Controls Checklist

The Positive Controls Checklist is a list of known positive privacy controls. When creating the checklist of positive controls, document both the positive and negative controls. In many cases, the negative control may only be "negative" based on the context in which it was presented. In practice, negative controls often may be used in a positive manner. For example, an organization that avoids the use of authentication techniques that can be easily replicated or "spoofed," such as caller ID, email addresses, or originating telephone numbers can result in the implementation of more stringent authentication techniques to prevent potential pretexting scams.

Research

To create these checklists, organizations need to research relevant commissioners' and regulators' findings, orders, guidelines, and papers to identify known risks and positive controls for the Business Activity selected. It is also advisable to access relevant case law, standards (recommended and mandatory), and best-practices papers from law firms, consulting firms, and solutions providers[13]. Internal sources, for example audit findings, would be another source.

This step of the PROP is very pragmatic. The PROP is focused directly on the Business Activity and on privacy for that specific area. The scope of the project will be scaled based on the resources available. The research identifies common and leading practices and allows the organization to identify creative approaches to compliance. The result for this phase is the

Nymity's Risk and Positive Control Checklists

The Office of the Privacy Commissioner of Ontario uses Nymity's risk and positive control checklists, as do hundreds of organizations around the world. Organizations using the Privacy Risk Optimization Process to implement Privacy by Design into their business practices can save hours of research time using these Risk and Positive Control Checklists. See appendix A for details.

[13] Nymity has identified over 400 sources of guidance for privacy management.

© Nymity Inc. 2009

completed risk and positive controls checklists to be used to create a Risk Optimization Plan.

Risk optimization works well for compliance as the threats related to non-compliance are generally very clear and the research identifies known vulnerabilities that could potentially be of risk to the organization. The research results in a solid understanding of the negative compliance risk and the baseline required for compliance. The compliance opportunities and positive controls for compliance found in this research phase are key to the creation of the Risk Optimization Plan.

Step 3: Create a Risk Optimization Plan

The project team uses the risk checklist to identify the positive and negative risks to their organization for each of the Business Activities. At this stage, the team includes all stakeholders, including the privacy office, Legal, IT, and the business unit. The team, reviewing the known risks from the checklist, conducts risk identification[14]. The result is a listing of identified risks to the organization, including opportunities which will enhance business practices. These risks are documented in the Risk Optimization Plan.

For the identified risks, the project team uses the Positive Controls Checklist to create a risk optimization plan that maximizes opportunities and minimizes threats and vulnerabilities. These controls are also documented in the Risk Optimization Plan. Some controls will address multiple risks and some may only partially address the identified risks.

At this stage, some organizations may elect to use traditional risk management procedures. For example, they may assess the likelihood of occurrence and impact for each risk and the cost of each of the controls. Organizations may assess the business advantage of going beyond compliance, inherent risk and residual risk. Users of the PROP are welcome to use these traditional risk management procedures, but they are beyond the scope of risk optimization and this paper.

During this stage, the project team may be tempted to divide documenting risks and controls into two separate steps. In practice, these steps quickly merge into a single planning exercise, ultimately blurring any attempt to work on risk first then controls. This is due to the project team trying to identify solutions when a problem is first identified. In other words, the project team will find positive controls as soon as a negative risk is identified. When an opportunity is found, there is also a tendency to find the relevant positive controls to take advantage of the opportunity. In fact, the opportunities often are the source for the positive controls that address the threats and vulnerabilities.

The PROP help organizations meet PbD Principle 2:

Privacy as the Default

One can be certain of one thing - the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, then their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

A question generally posed at this time is: “Will the PROP miss a compliance requirement?” In practice, compliance requirements are not missed because the research phase would include the law and any regulatory supporting documents which detail the legal considerations. If it is a new law, and thereby not having any regulatory actions or case law, the research is best focused on legal briefs from law firms and documents from other learned experts. In practice,

[14] ISO/IEC Guide 73:2002. Risk Identification is the process to find, list and characterize element of risk.

© Nymity Inc. 2009

there is a wealth of data available, even for newly enacted legislation, and it is unlikely a risk will be missed.

Another question asked is: "What about concepts like the reasonableness test, when complying with laws that are not prescriptive?" This is where the PROP provides relevant data so that the project team can make an informed decision about what is reasonable. For prescriptive laws, the PROP can provide creative compliance solutions.

In addition to creating a Risk Optimization Plan containing actions the organization will undertake to optimize the privacy risk, Step 3 also fosters a good working relationship between the privacy office and the business unit. This helps ensure the organization will take advantage of future opportunities to implement privacy into their business practice.

A partial Positive Controls Checklist is provided as an example in Appendix C.

Step 4: Implement the Risk Optimization Plan

Implementing the resulting Risk Optimization Plan will typically see changes in the short-term, medium-term, and long-term.

1. Short-Term: Some of the positive controls identified will be implemented almost immediately during the Create Risk and Positive Control Checklists step. It is not uncommon for somewhat simple controls to be implemented right away, thus providing instant value. For example, a simple change to the call script in the customer authentication process that provides better customer service and improves customer privacy may be implemented immediately (if it does not require a change in policy).

2. Medium-Term: The optimization plan will likely include updating the relevant operational policies and procedures, training employees, and updating call scripts, brochures, notices, and contracts. These may take a few weeks to have modified, approved, and implemented.

3. Long-Term: The optimization plan may go beyond creating or updating policies and procedures and identify positive controls that require more time to implement. Often, controls that are based on IT infrastructure changes or software application modifications take time. For example, it might be identified that the customer relationship management system (CRM) which the call-centre employees use for customer authentication could be updated to include an enhancement that would increase the efficiency of the customer authentication process and provide another layer of privacy options for customers. These changes to the CRM may be scheduled for the next release of the software, which could be scheduled six or ten months in the future.

The PROP help organizations meet PbD Principle 3:

Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, or 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.

© Nymity Inc. 2009

Section 4: Dispelling the Myths

The most important benefit of using the PROP is that this privacy management method helps organizations implement privacy without constraining the business practices. The PROP's focus on opportunities and positive privacy controls enables organizations to implement the guiding principles of Privacy by Design. Some of the other benefits of the methodology include that it is:

1. **Tactical** – the PROP is granular in nature as it provides specific guidance for business activities. It provides a bottom-up approach to privacy management, which solves specific problems.
2. **Scalable** – the PROP works for small projects or large complex projects. It scales based on the amount of resources allocated and the business' needs.
3. **Efficient** – the PROP does not require a great deal of training, questionnaires, detailed spreadsheets, software, large work plans, or a large team of experts.
4. **A Pragmatic Compliance Enabler** – the PROP provides an effective and pragmatic alternative to the traditional approaches to complying with privacy and data protection laws.
5. **Key for Implementing Effective Policies** – the PROP provides an effective approach for implementing corporate privacy policies into business practices. It helps an organization put privacy principles into practice.
6. **Sources Common and Leading Practices** – the PROP allows the organization to take advantage of the wealth of knowledge and expertise available to gain an understanding of common and leading practices, providing creative approaches to compliance.
7. **Complementary to Traditional Approaches** – the PROP works with traditional approaches to privacy management including privacy assessment, privacy audits, and privacy impact assessments (PIAs) as a complementary tool that facilitates positive risk mitigation strategies.
8. **Opportunistic** – the PROP uncovers areas to enhance operations. It allows an organization to exploit the wealth of knowledge and expertise relevant to specific areas of concerns.

The PROP eradicates the myths discussed in the beginning of the paper. PROP addresses:

☑ "*Privacy constrains business operations"* – the PROP does not include gap assessments and mitigation strategies which inherently result in restrictive controls being placed on operations. Instead, it provides organizations with the ability to build privacy into their business practices without restrictions;

☑ "*Privacy is nothing more than compliance*" – the PROP presents opportunities for organizations to go beyond pure compliance, with these opportunities being mutually beneficial to both business practice and privacy;

☑ "*Implementing privacy controls will be expensive*" – the PROP enables organizations to find and implement positive controls that are cost-effective and result in positive returns on that investment.

Ultimately, the PROP focus on opportunities and positive privacy controls makes it a pragmatic process for implementing privacy into operational policies and procedures, which results in the implementation of Privacy by Design for business practices.

© Nymity Inc. 2009

Appendix A: Nymity's PbD Risk and Control Checklists

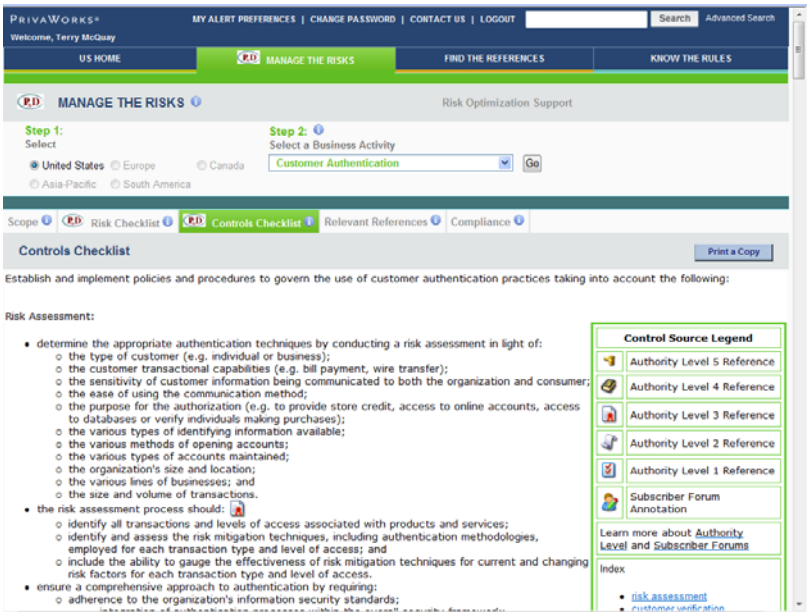
Nymity is a global privacy and data protection research services firm specializing in compliance and operational risk management. Nymity is best known for its world-leading research tool, PrivaWorks, now used by over 1,000 privacy professionals. PrivaWorks is a web-based research tool for privacy professionals. Nymity's research spans across the United States, Europe, and Canada, and will include Asia-Pacific and South America in 2010.

Risk Optimization Background

Nymity developed and has been using risk optimization as an integral part of its research for many years. In the summer of 2009, Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada asked Nymity to publish its once-proprietary research process and make it publicly available to help organizations build privacy into their business practices. Nymity honoured the Commissioner's request, which is the genesis of this joint paper. Nymity research includes creating and making available to PrivaWorks subscribers:

Risk Checklists - known threats and vulnerabilities for each business activity; and

Positive Control Checklists - known positive privacy controls for each business activity.



The checklists support privacy management activities, including:

- Developing operational policies and procedures;
- Developing Privacy Officers education;
- Creating content for employee training programs;
- Creating mitigation strategies for privacy audits and PIAs;
- Creating content for executive presentations; and
- Using the Privacy Risk Optimization Process introduced in this paper.

Nymity invests over 100 hours of legal research for each business activity to create the checklists. The checklists are made available to subscribers of Nymity's research tool, PrivaWorks. Learn more by visiting www.nymity.com.

© Nymity Inc. 2009

Appendix B: Privacy by Design Principles

Privacy by Design is a concept developed in the 90's by Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems. Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks. Rather, privacy assurance must ideally become an organization's default mode of operation. Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, it is understood that a more substantial approach is required: extending the use of PETs to taking a positive-sum (win/win)—not a zero-sum (win/lose)—approach.

Privacy by Design now extends to a trilogy of encompassing applications:

1. IT systems;
2. Accountable business practices; and
3. Physical design and infrastructure.

Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy protection requirements tend to be commensurate with the sensitivity of the data.

Seven Principles of Privacy by Design

The objectives of Privacy by Design—ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage—may be accomplished by practising the following principles:

1. **Proactive not Reactive; Preventative not Remedial**
   The Privacy by Design (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 them from occurring. In short, Privacy by Design comes before the fact, not after.

2. **Privacy as the Default**
   One can be certain that the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3. **Privacy Embedded into Design**
   Privacy by Design is embedded into the design and architecture of IT systems and business practices. 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.

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

© Nymity Inc. 2009

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. **End-to-End Lifecycle Protection**
   Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, and in a timely fashion. Thus, Privacy by Design ensures cradle-to-grave, lifecycle management of information, end-to-end.

6. **Visibility and Transparency**
   Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent to users and providers alike. Remember: trust but verify.

7. **Respect for User Privacy**
   Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

© Nymity Inc. 2009

Appendix C: Example of PROP Positive Privacy Controls

Below is a partial example of positive privacy controls for the business activity "Customer Authentication"[15]:

1. determine the appropriate use of the four different factors of authentication:
   - something the individual "knows":
     - a PIN;
     - a password — types include:
       - passwords created by the user;
       - passwords that are machine generated;
       - half and half:
         - uses a word that the user chooses and combines it with a nonsense syllable generated by the machine or network administrator.
       - passphrases:
         - a combination of words, e.g. "I was tall when I was twelve";
         - numbers can also be added inside the passphrase e.g. "my favorite rock group is U2".
         - can be a line from a favorite song, a proverb learned as a child or the punch line of a joke;
         - can be a passphrase acronym:
           - the user comes up with a sentence, then creates an acronym from it to use as the password.
       - customer-selected images that must be identified or selected from a pool of images;
     - Knowledge-Based Authentication (KBA) methods - consumers are identified by answering a set of questions only they could reasonably be assumed to know, e.g.:
       - asking for the person's date of birth, mother's maiden name or favorite color:
         - does not exemplify personal facts that are that secret or difficult to obtain;
         - may be sufficient verification for a website without any non-public PII.
       - asking whether there is a co-signer on a particular loan, the name of a work colleague or old college roommate:
         - correct responses are more difficult to verify by an imposter while still reasonably memorable for the correct person.
       - an out-of-hand mechanism to which an imposter is presumed not to have access, e.g.:
         - depositing a small amount into the user's bank account and ask the user for the amount deposited.
   - something the individual "has":
     - bank card;
     - smart card;
     - USB token device;
     - password-generating token — which produces a unique one-time password ("OTP") each time it is used:
       - the customer enters the user name and regular password followed by the OTP generated by the token.
     - OTP security cards;
     - digital certificate using public key infrastructure where each customer has a:
       - public key — made available to those who need to verify the customer's identity; and

> Note to Reader:
>
> This example of positive controls is a small subset of controls available. In some cases the controls listed are positive based on how they are implemented. This example is not provided to be used for privacy management as it is incomplete.

[15] This example is a small subsection from PrivaWorks Customer Authentication PbD Controls Checklist. Do not use without the other sections.

© Nymity Inc. 2009

- private key — stored on the customer's computer or a separate device such as a smart card- which:
  - creates an electronic identifier called a digital signature that:
    - uniquely identifies the holder of a private key; and
    - can only be authenticated with the corresponding public key.
- scratch cards — containing numbers and letters in a grid format:
  - the customer enters the user name and password and then will be asked to input the characters contained in a randomly chosen cell in the grid.

- something the individual "is," for example:
  - facial scan
  - fingerprint — digital or ink;
  - voice pattern;
  - keystroke recognition;
  - handwriting recognition;
  - dynamic signature verification:
    - multiple biometric characteristics of a signature are scrutinized and compared against a reference signature kept on file.
  - finger and hand geometry;
  - retinal scan;
  - iris scan;
  - palm vein scan.
- additional authentication methods, including:
  - Internet Protocol Address ("IPA") verification:
    - software products are available that:
      - identify and analyze data elements (e.g. location, domain name); and
      - check it against multiple data sources and profiles to prevent unauthorized access.
    - the user is authenticated if the IPA and the profiled characteristics of past sessions match information stored for identification purposes,
  - geo-location verification:
    - determines a user's cyberspace distances and compares them with cyberspace distances for known locations:
      - if the comparison is considered reasonable, the user's location can be authenticated.
  - voice-enabled passcode:
    - random passcode sent via voice call to user's handset.
  - mobile credentials:
    - stand-alone application residing on phone, capable of generating a OTP; or
    - short message service OTP:
      - one-time password delivered by text to a user's handset.

© Nymity Inc. 2009

Appendix D: About the Authors

Terry McQuay
President
Nymity Inc.

Terry McQuay is president and founder of Nymity, a global privacy and data protection research firm best known for its research tools for privacy professionals. Terry is CIPP and CIPP/C certified, is a Fellow for the Ponemon Institute, is on the Advisory Council for The Future of Privacy, resides on one of IAPP's Boards, is co-chair of an IAPP KnowledgeNet, and frequently delivers IAPP Privacy Bootcamps and CIPP Foundations Training. He is an active speaker on a variety of topics ranging from privacy compliance to risk management at privacy conferences, and is also the creator of the PbD Risk Management Methodology, a tactical, operational risk management process based on the principles of Privacy by Design.

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

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is protected in Ontario – and around the world. Dr. Cavoukian is Ontario's first Information and Privacy Commissioner to be re-appointed for an unprecedented third term. Initially appointed in 1997, her role in overseeing the operations of the freedom of information and privacy laws in Canada's most populous province has been extended to 2014. Like the Auditor General, she serves as an Officer of the Legislature, independent of the government of the day.
Noted for her seminal work on Privacy Enhancing Technologies in 1995, her mantra of "privacy by design" seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protections. Dr. Cavoukian also serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, in Canada.

Dr. Cavoukian's published works include Who Knows: *Safeguarding Your Privacy in a Networked World* (1997), written with Don Tapscott, and, *The Privacy Payoff: How Successful Businesses Build Customer Trust* (2002), written with Tyler Hamilton.

© Nymity Inc. 2009