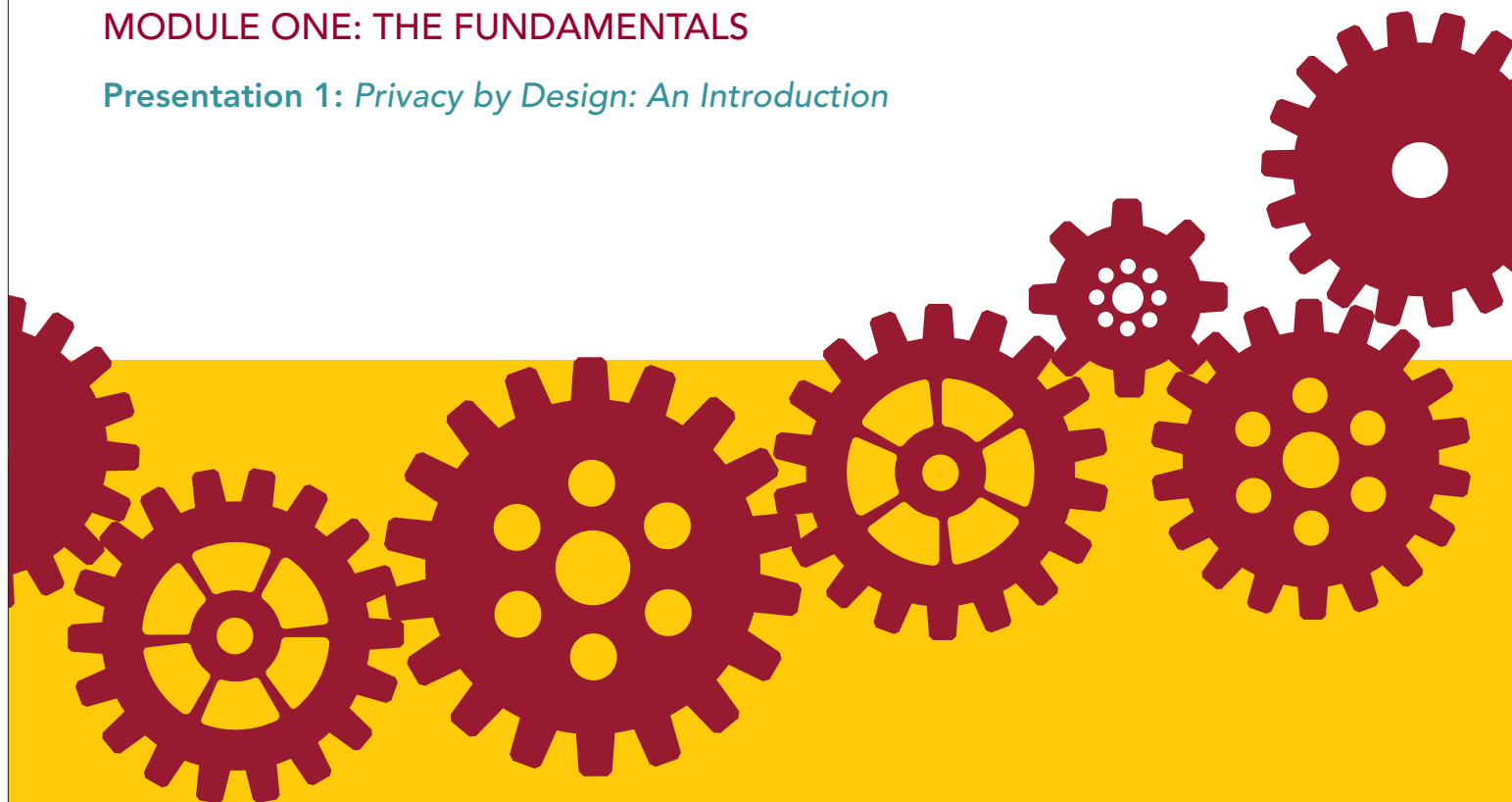


Privacy by Design Curriculum 2.0

Instructor Resources

MODULE ONE: THE FUNDAMENTALS

Presentation 1: *Privacy by Design: An Introduction*



CONTENTS

Overview	2
Essential Reading	2
Learning Objectives	2
<i>Privacy by Design: Overview of Presentation</i>	3
Further Reading	4
Presentation Materials with Instructor Notes	6



Overview

This section introduces the concept of privacy as informational self-determination. It summarizes Fair Information Practices and provides an overview of the business case for privacy and data protection.

It explains the outdated zero-sum view of privacy as being in conflict with other objectives, and offers an alternative, positive-sum paradigm. The 7 Foundational Principles of *Privacy by Design* are presented, along with an overview of the benefits of building privacy into the development process, from the outset.

Essential Reading

Ontario Information and Privacy Commissioner, [Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices](http://www.privacybydesign.ca).
www.privacybydesign.ca

Learning Objectives

Participants will develop an understanding of privacy as informational self-determination, and be able to identify how protecting privacy can help support business success by building trust. Participants will also be able to describe the benefits and characteristics of the Privacy by Design approach, and its 7 Foundational Principles.

Privacy by Design: An Introduction

Overview of Presentation

Slide	Title	Theme
1.1	What is Privacy?	Informational self-determination
1.2	Fair Information Practices	How privacy has traditionally been protected
1.3	Privacy as a Business Issue	Privacy has yet to peak
1.4	The Privacy Payoff	How trust fuels brand loyalty and yields competitive advantages
1.5	The Perils of Ignoring Privacy	Challenges awaiting organizations that do not take privacy seriously
1.6	Market Leaders are Paying Attention!	How the privacy marketplace is changing
1.7	<i>Privacy by Design</i>	What is <i>Privacy by Design</i> ?
1.8	Breaking with Tradition: The Zero-Sum Paradigm	The outdated notion that privacy is in conflict with other values and objectives
1.9	A New Perspective on Privacy	The positive-sum approach
1.10	<i>Privacy by Design</i> : Overview	An overview of the 7 Foundational Principles and the areas where they apply
1.11	Principle One	Proactive, not Reactive
1.12	Principle Two	Privacy as the Default
1.13	Principle Three	Privacy Embedded into Design
1.14	Principle Four	Full Functionality
1.15	Principle Five	End-to-end Security – Lifecycle Protection
1.16	Principle Six	Visibility and Transparency
1.17	Principle Seven	Respect for User Privacy
1.18	Operationalizing <i>Privacy by Design</i>	Including privacy in the project lifecycle process
1.19	How PIAs Can Help	Privacy Impact Assessments
1.20	The Ultimate Goal	Embedding <i>PbD</i> in the Organization

Further Reading

What is Privacy?

Alan Westin, *Privacy and Freedom*. Atheneum (1967).

Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*. Harvard Law Review 4, 193-220 (1890)

The Business Case for Privacy

Ann Cavoukian, Ph.D., Tyler Hamilton, *The Privacy Payoff: How Successful Businesses Build Consumer Trust*. McGraw-Hill Ryerson, 2002.

Information Commissioner's Office (U.K.), [The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection](http://www.ico.gov.uk). www.ico.gov.uk

Fair Information Practices

Information and Privacy Commissioner, Ontario, [Creation of a Global Privacy Standard](http://www.ipc.on.ca). www.ipc.on.ca

OECD, [Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](http://www.oecd.org). www.oecd.org

European Union, [Directive 95/46/EC](http://www.eur-lex.europa.eu). www.eur-lex.europa.eu

Canadian Standards Association's [Model Code for the Protection of Personal Information](http://www.csa.ca). www.csa.ca

Privacy by Design

Ontario Information and Privacy Commissioner, [Privacy by Design: The 7 Foundational Principles](http://www.privacybydesign.ca). www.privacybydesign.ca

Ontario Information and Privacy Commissioner, [Landmark Resolution passed to preserve the Future of Privacy](http://www.privacybydesign.ca). www.privacybydesign.ca

Centre for Democracy and Trust (CDT), Report: [The Role of Privacy by Design in Protecting Consumer Privacy](http://www.cdt.org). www.cdt.org

European Data Protection Supervisor, [Opinion on privacy in the digital age \(March 2010\): Privacy by Design" as a key tool to ensure citizens' trust in ICTs](http://www.edps.europa.eu). www.edps.europa.eu

Julian Sanchez, *The Trouble with "Balance" Metaphors*. www.juliansanchez.com (Blog posting February 4, 2011)

Privacy Impact Assessments

Information and Privacy Commissioner, Ontario, Canada. [Privacy Diagnostic Tool](#).
www.ipc.on.ca

Information and Privacy Commissioner, Ontario, Canada. [The New Federated Privacy Impact Assessment \(F-PIA\)](#). www.ipc.on.ca

Office of the Privacy Commissioner of Canada. [PIPEDA Self-Assessment Tool](#).
www.priv.gc.ca

Information Commissioner/UK, [Privacy Impact Assessments: An International Study of their Application and Effects](#). www.ico.gov.uk

Information Commissioner/U.K., [PIA Handbook Version 2.0](#). www.ico.gov.uk

Office of the Privacy Commissioner/Australia, [Privacy Impact Assessment Guide](#).
www.privacy.gov.au

Presentation Materials with Instructor Notes



Slide 1

What is Privacy?



Slide 2

Conceptually speaking, there are a few different types of privacy (e.g. physical privacy, workplace privacy). Our focus here is on *information privacy*, which Alan Westin described in his famous book, *Privacy and Freedom*, as “the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others.”

Many organizations need to manage – which means collect, use and disclose – some personal information about their customers, employees, vendors, and others in order to conduct their business. Personal information is any recorded information about an identifiable individual. It can include the individual’s name, address, sex, age, education, medical or employment history – and a great deal of other information that can be linked to that individual, like opinions, habits, and behaviors.

Informational self-determination is the vehicle through which information privacy is achieved. It is also the basis of modern privacy laws and practices around the world.

Protecting Privacy: Fair Information Practices

1. Consent
2. Accountability
3. Identifying Purposes
4. Collection Limitation
5. Use, Retention and Disclosure Limitation
6. Accuracy
7. Security
8. Openness
9. Access
10. Compliance

Source: Global Privacy Standard

Slide 3

Informational self-determination is realized through Fair Information Practices (FIPs), which have existed since the early 1980s, and are the foundation of data protection practices in most jurisdictions.

There are many versions of FIPs, different in subtle ways, but they generally reflect these same core concepts.

The version shown here is based on the Global Privacy Standard, which was developed by a Working Group of international Data Protection Commissioners chaired by Ontario Commissioner Dr. Ann Cavoukian in 2006. The Global Privacy Standard uses the Canadian Standards Association's Model Code for the Protection of Personal Information as its foundation.

Privacy as a Business Issue

“Anyone today who thinks the privacy issue has peaked is greatly mistaken... We are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope.”

Forrester Research, 2001

www.privacybydesign.ca

Slide 4

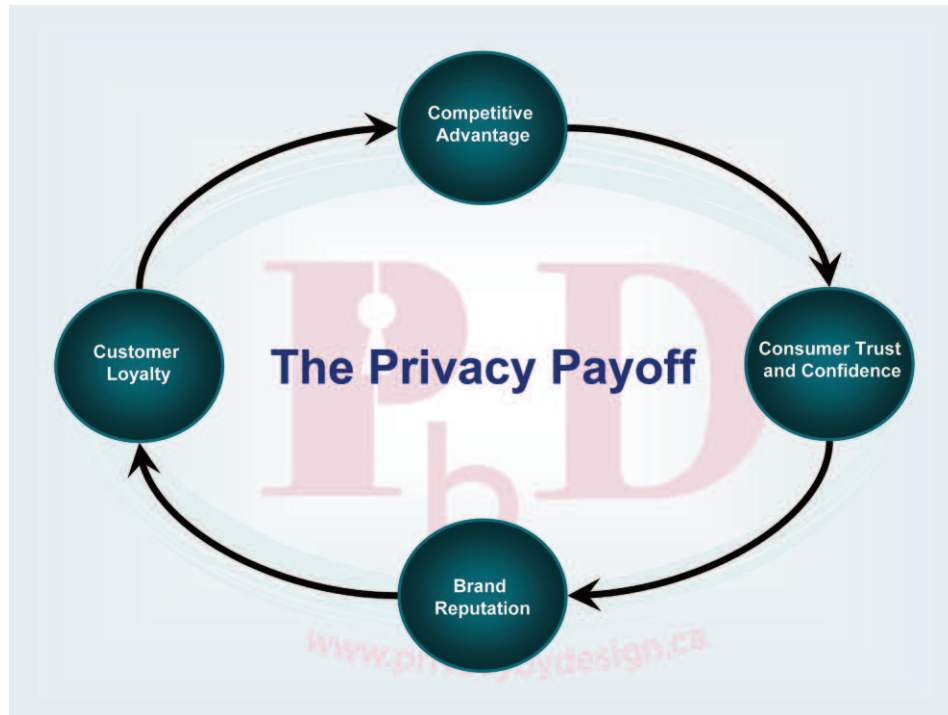
While much of the focus in the early days of privacy was on preventing the collection of personal information by governments, in 2001, Forrester Research issued this prescient warning to business.

It was based on the recognition that from a business perspective, privacy is a consumer trust issue.

Appropriate management of personal information is an important aspect of establishing and maintaining trust in the digital economy. Failure to manage it, or mismanagement of it, can have profound economic implications.

Today, there is plenty of evidence that Forrester’s prediction was right.

For organizations that handle personal information and depend on consumer trust for their success, there is no longer any doubt that privacy matters.



Slide 5

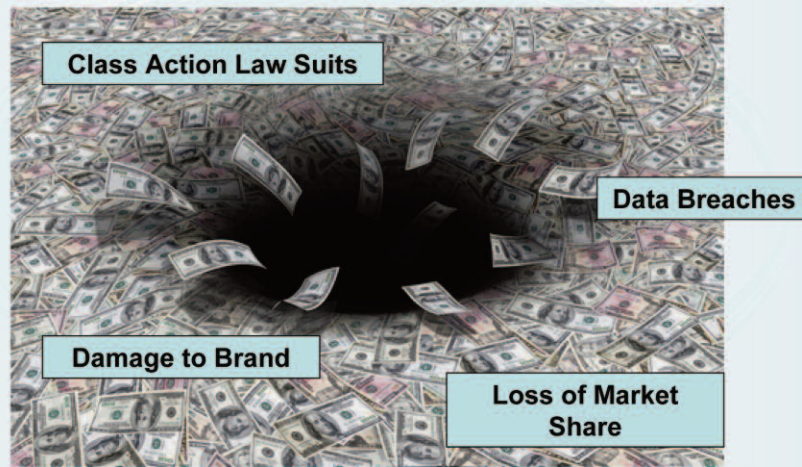
Why does privacy matter? Increasingly, privacy matters to business because it matters to consumers.

The business case for privacy focuses, in essence, on gaining and keeping consumer trust, helping drive loyalty and repeat business, and avoiding “churn.”

The diagram above shows how the value proposition for online privacy typically breaks down:

- Consumer trust is among the drivers of successful customer relationship management and lifetime value;
- Consumer trust hinges critically on the strength and credibility of an organization’s information privacy policies and practices;
- Positive experiences reinforce trust in the brand; and
- Trusted brands attract customer loyalty, which drives successful customer relationship management and creates competitive advantages.

The Perils of Ignoring Privacy



Slide 6

If the link between privacy and trust is not enough to motivate action, then there are many other reasons for organizations to take privacy seriously.

The flip side of the Privacy Payoff is the host of challenges that organizations can face when they fail to protect personal information. Experience has shown that waiting until you have a privacy problem, and then taking steps to fix it, can be extremely costly.

Once privacy has been lost, and trust has been broken, then organizations can expect to face hard and soft costs associated with:

- Legal liabilities, class action suits;
- Loss of client confidence and trust;
- Diminution of brand and reputation;
- Loss of customers, competitive edge;
- Penalties and fines levied;
- Costs of crisis management, damage control, review and retrofit of information systems, policies and procedures.

Indeed, a U.S. study found that the cost of a data breach is about \$214 per record and is on the rise. (*Ponemon Institute*)

Market Leaders are Paying Attention!

Profound shift in privacy management in the US from 1995 to 2010:

- Thousands of companies have now created Chief Privacy Officer (CPO) positions
- “Privacy has evolved over the last several years to be defined in large part by respect for what consumers expect regarding the treatment of their personal sphere.”

Kenneth A. Bamberger & Deirdre K. Mulligan,
Privacy on the Books and on the Ground

www.privacybydesign.ca

Slide 7

The combined effect of these factors has been a recognition among market leaders that privacy is an important business issue and that it is linked to both risk management and competitive advantage.

At the same time, there has been an expansion – driven by experience with consumer expectations about how their personal information will be managed – in how organizations understand privacy. In this environment, it is becoming clear that FIPs can no longer be the end goal; they are the starting point.



Slide 8

That's where *Privacy by Design* comes in.

Privacy by Design is an approach to engineering privacy directly into the design of new technologies, business processes, and networked infrastructure as a part of the core functionality.

It advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks or Fair Information Practices; rather, privacy assurance must ideally become an organization's default mode of operation.

By practicing *Privacy by Design*, organizations can better align themselves with shifting consumer expectations about how their personal information should be managed in our increasingly data-rich society.



Slide 9

PbD breaks significantly with traditional approaches to privacy protection.

In many organizations, for example, privacy has been seen as being in CONFLICT with other goals, especially business goals, and the relationship has been seen as a zero-sum one, where greater privacy protection necessarily means less security or diminished performance (or a decrease in some other essential dimension).

Balance metaphors, where people speak in terms of the need to balance privacy against other values, arise from this paradigm. These types of metaphors are often heard in the context of discussions about security, for example. This is what lies at the heart of the claim that citizens must give up a certain amount of privacy in order to have increased security.

When privacy is pitted against other values in this model – when the choice becomes privacy OR security, or privacy OR functionality – then privacy often takes second place.

A New Perspective on Privacy: The Positive-Sum Paradigm

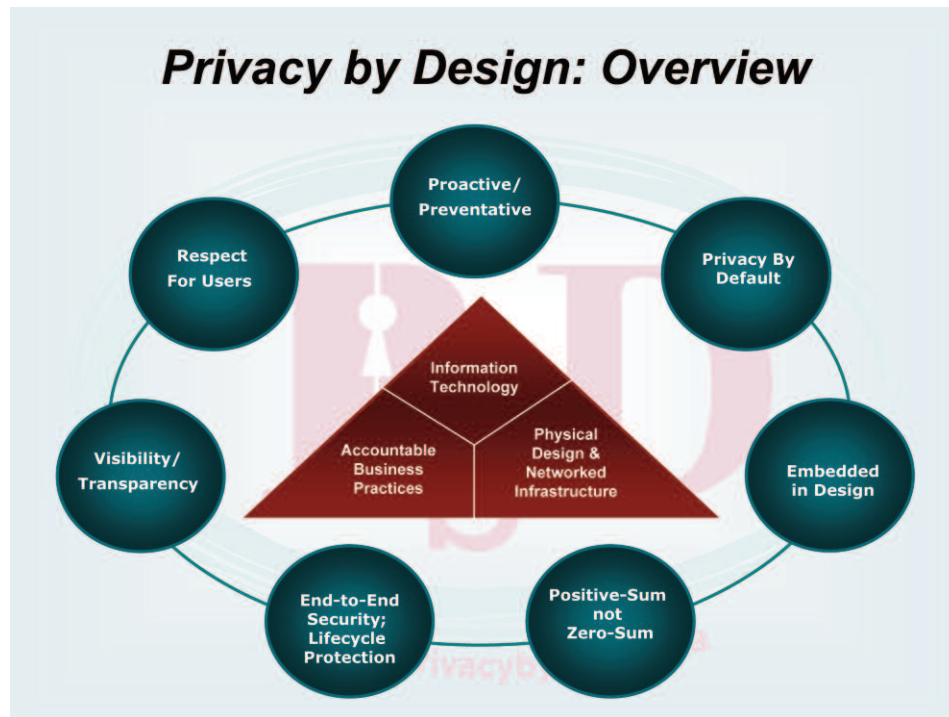


www.privacybydesign.ca

Slide 10

When we look at privacy through the lens of a positive-sum paradigm, however, we see that a win-win is possible. We can have more security AND more privacy. More efficiency AND more privacy. And so on.

How? By proactively building privacy into the system, engineering it into the technology or business process right from the outset. That's the essence of *Privacy by Design*, and its effect is to minimize the unnecessary collection and uses of personal data by the system and its operators, strengthen data security, and empower individuals to exercise greater control over their own information. The result is a system that achieves both functionality and privacy – a win-win outcome.



Slide 11

Privacy by Design is expressed through 7 Foundational Principles, the application of which support positive-sum outcomes.

These 7 Principles (shown here in the bubbles) may be applied to a trilogy of application areas:

Technology – Building privacy directly into technology and networked infrastructure, at the earliest developmental stage;

Accountable Business Practices – Incorporating privacy into competitive business strategies and operations;

Physical Design and Networked Infrastructure – Ensuring privacy in physical settings, such as hospitals and pharmacies.

In all of these environments, *Privacy by Design* enables achievement of business and project objectives, while ensuring that personal information is managed appropriately.

Let's look at each principle in detail.



Slide 12

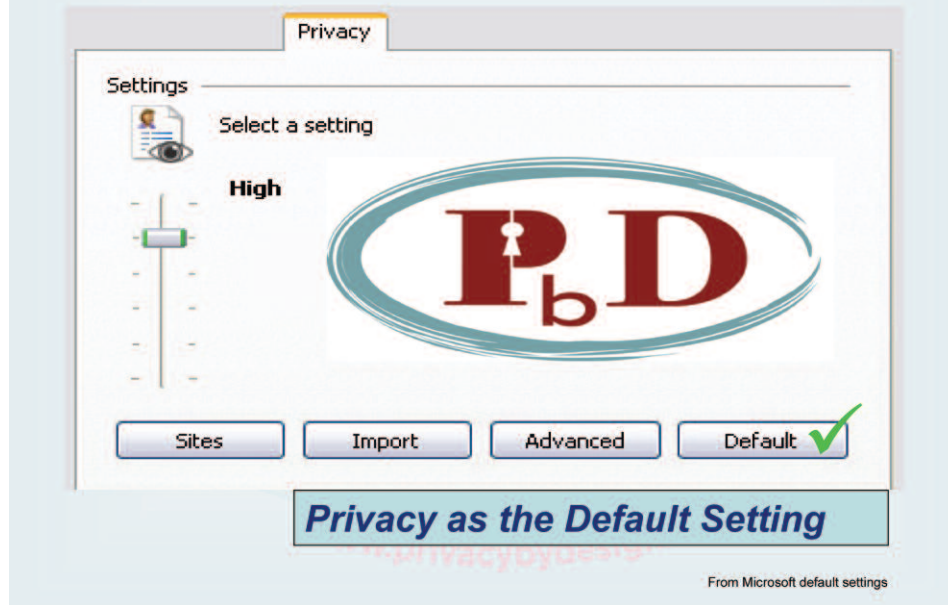
1. Proactive not Reactive; Preventative not Remedial

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.

This implies:

- A clear commitment, at the highest levels, to set and enforce high standards of privacy – generally higher than the standards set out by global laws and regulation.
- A privacy commitment that is demonstrably shared throughout by user communities and stakeholders, in a culture of continuous improvement.
- Established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways.

Principle Two

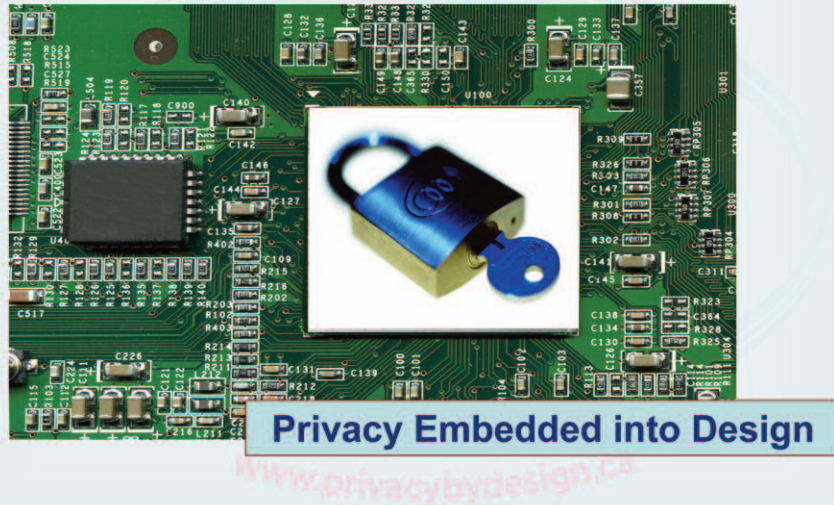


Slide 13

2. Privacy as the Default Setting

We can all 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, 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*.

Principle Three



Slide 14

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, and is delivered without diminishing functionality.

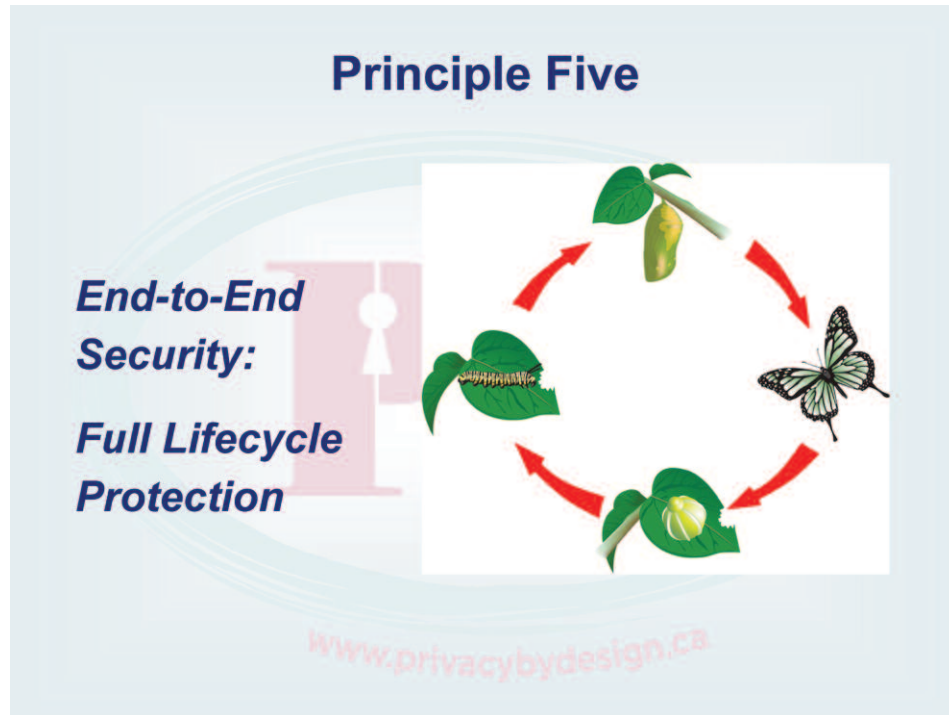
Principle Four



Slide 15

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 possible to have both.



Slide 16

5. End-to-End Security — Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

Principle Six



Slide 17

6. Visibility and Transparency — Keep it Open

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.

Principle Seven

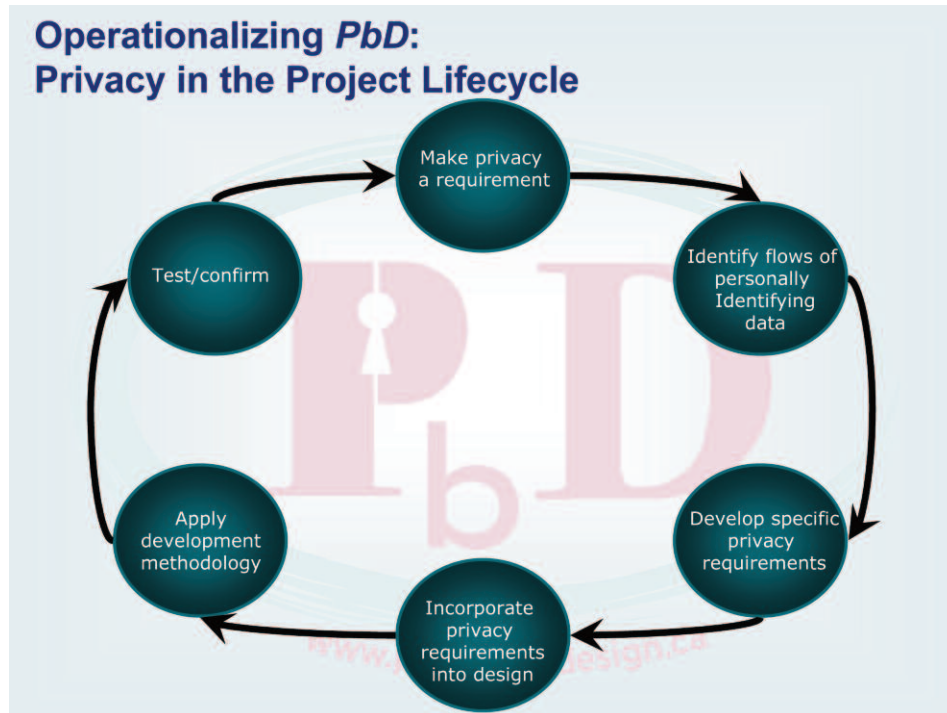


Respect for User Privacy

Slide 18

7. Respect for User Privacy — Keep it User-Centric

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.



Slide 19

Giving life to the principles of *Privacy by Design* means applying them in a variety of contexts.

At the project level, the idea of building privacy in at the design phase does not imply that your development **PROCESS** needs to change. Whatever processes you use in your organization to develop IT systems, business practices, or physical design, can continue to be used.

What changes is that, at the outset, you have to make privacy a requirement.

Then, in order to make that requirement meaningful, you have to identify how personal information is, and might be, collected, used, or disclosed and discarded by the new system or process. As you do this mapping, ask yourself if your business objectives really require all of the personal information that you are contemplating collecting, using, or disclosing. Data minimization is an important concept to be bringing in at the earliest stages.

Once you understand the personal data flows, you can develop specific privacy requirements based on the principles of *Privacy by Design*, which we will look at in a moment.

Incorporating those principles and working through your development methodology, you can then test and confirm the design as usual.

How PIAs Can Help

- **Privacy Impact Assessment (PIA)**
 - Risk management tool that identifies the actual or potential effects of a proposed or existing system, technology, or program
 - Promotes systemic analysis of privacy issues
 - Supports informed decision-making
 - Early warning device
 - May reduce costs

www.privacybydesign.ca

Slide 20

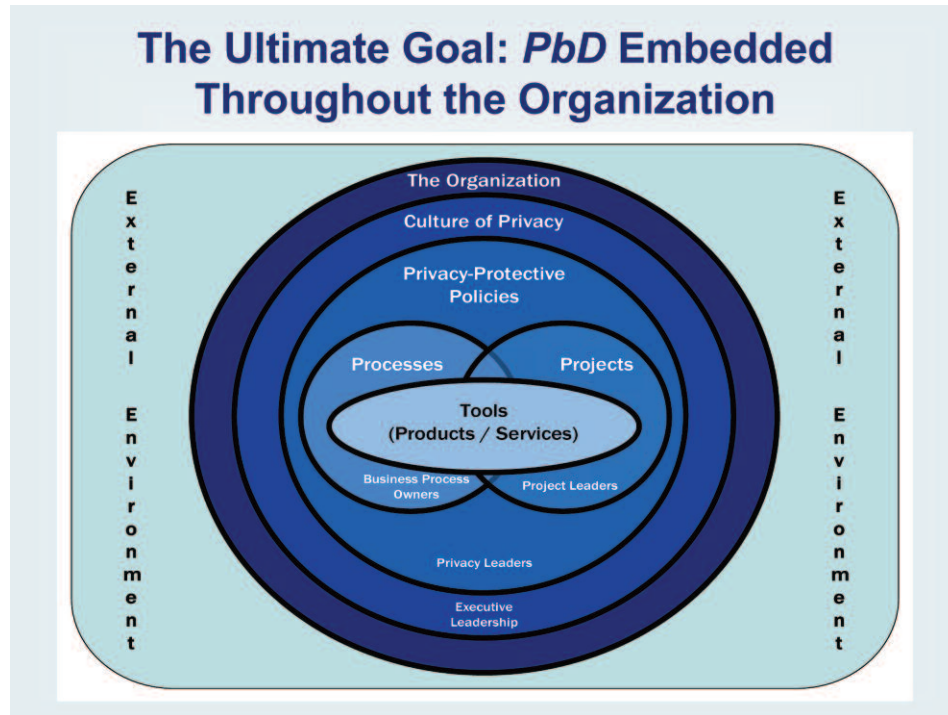
As they engage in the development process, organizations may find it useful to conduct a full or partial Privacy Impact Assessment.

For some time now, Privacy Impact Assessments (PIAs) have been the principal resource for organizations with privacy compliance programs wanting to either design privacy into new systems and processes or assess existing ones. A PIA is a formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology, or program may have on an individual's privacy. A PIA also identifies ways in which privacy risks can be mitigated.

The PIA process consists of developing an information flow map, applying a set of privacy questions to the information flow, identifying risks, and developing an approach to managing these risks. A PIA is generally modular in nature and involves people from throughout an organization, since most policies, governance frameworks and systems are neither the purview nor the expertise of a single person.

PIAs offer a number of benefits, including supporting informed decision-making and system design, anticipating the public's possible privacy concerns, and generating confidence that privacy objectives are being considered and addressed in the development and implementation of new systems and processes.

When a PIA is being used as a design tool, it must be approached as a living document, one that will be used and revised many times throughout the design and implementation process.



Slide 21

Operationalizing the 7 Foundational Principles on *PbD* on a project basis is one step toward the ultimate goal: having *PbD* embedded throughout the organization's governance and operations.

Full implementation begins with the organization's executive leadership, which sets the tone of the organization's operations. It is within this realm that the opportunity exists to create what our office has termed a **Culture of Privacy**. Such a culture enables sustained collective action by providing people 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.

Inevitably, a Culture of Privacy fosters the development of privacy-protective **policies**. Informed by senior management's perspective on risks and opportunities (the forces of the external environment), well-implemented policies will form a governance structure and serve to institutionalize privacy practices.

Processes are multi-use constructs, frequently manifested as tools or checklists, which ensure that everyone within the organization, simply by following the steps, will fall within the bounds of a given policy.

Closely related to process and, in fact, frequently overlapping it, are **projects**. Generally speaking, projects are undertaken under the auspices of organizational policy. Often, their execution is facilitated by any number of organizational processes. For many, the project is the place where the “rubber” of privacy hits the proverbial road. It is where committed professionals take the issue by the horns, ensuring that privacy is a fundamental dimension of their work.

That brings us to the innermost circle of the diagram above: tools. Tools include a broad collection of resources which facilitate either or both processes and projects. Many of them may be described as necessary, but not sufficient, to ensure end-to-end privacy protectiveness. They include:

- Privacy Impact Assessments and staff education modules;
- Privacy-Enhancing Technologies – which may or may not be inherently privacy protective, like: biometric encryption, RFIDs, and drive encryption technology;
- Services, such as certification regimes (like the *Euoprise* European Privacy Seal and Japan’s *PrivacyMark* or Deloitte’s “PBD” Assessment Methodology).

**More information and a growing
library of resources are available at**
www.privacybydesign.ca

Slide 22