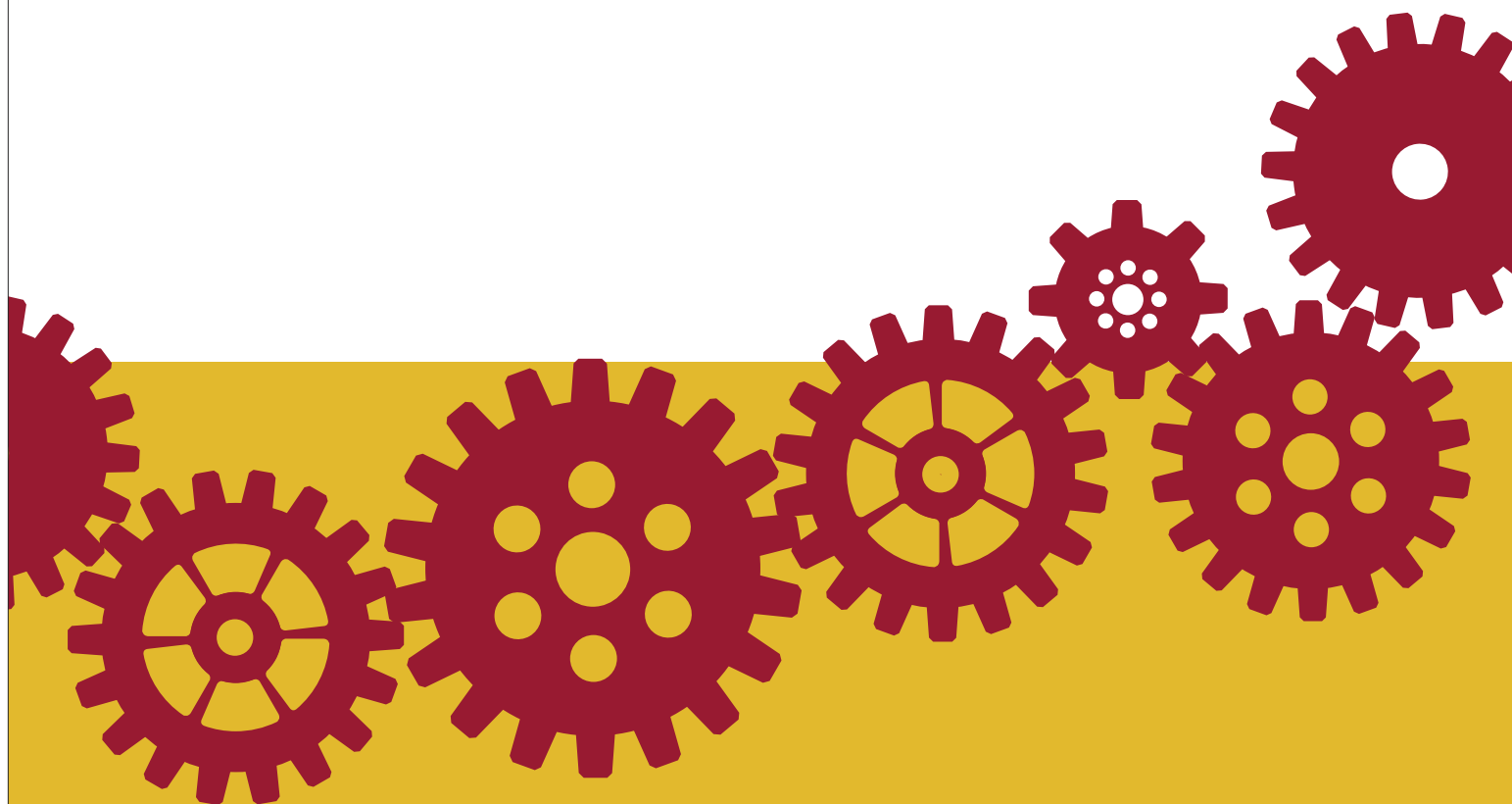


Privacy by Design Curriculum 2.0

Instructor Resources

OVERVIEW



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

Table of Contents

Instructor Resources

Welcome	3
Introduction	4
Using this Curriculum	5
Course Overview	6

Course Materials

Module One: The Fundamentals	6
Presentation 1: <i>Privacy by Design</i> : An Introduction	6
Presentation 2: <i>Privacy by ReDesign</i> : Building a Better Legacy.....	7
Module Two: Applied Privacy by Design	8
Presentation 3: Applied <i>Privacy by Design</i> : The Smart Grid	8
Presentation 4: Applied <i>Privacy by ReDesign</i> : Embedding Privacy in Organizational Culture, Policy, and Process	9
Presentation 5: Applied <i>Privacy by ReDesign</i> : Biometric Encryption	10

Welcome

Welcome to the Privacy by Design Curriculum 2.0!

Like its predecessor, this curriculum is designed to introduce *Privacy by Design (PbD)* – an approach to protecting privacy by embedding it into the design specifications of information technologies, accountable business practices, and networked infrastructures, right from the outset.

This update of the *PbD* Curriculum makes it easier to use, and provides expanded instructor resources, essential readings, and more practical examples of how *PbD* is being implemented in key sectors. We have also consolidated some of the material, and added a section on *Privacy by ReDesign* – a new approach to applying the 7 Foundational Principles of *Privacy by Design* to existing and legacy systems.

This Curriculum continues to be a work in progress. Please share your comments and suggestions with us at info@ipc.on.ca.

Introduction

Privacy by Design was developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, in the 1990s, as a response to the growing threats to online privacy that were beginning to emerge at that time.

It represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches, after-the-fact. Alexander Dix, Berlin Commissioner for Data Protection and Freedom of Information, has described these traditional approaches as "locking the stable door after the horse has bolted."¹

By contrast, *PbD* requires that organizations think about privacy proactively, from the initial development phases of systems and processes.

Over the past several years, *Privacy by Design* has been steadily gaining recognition and acceptance, and is fast becoming the gold standard for privacy, around the world. It is increasingly important for forward-thinking organizations – and everyone in them, from the engineers to the risk managers and the senior executives – have a solid understanding of what privacy protection means today.

These course materials are designed to do just that. While the modules build on one another for audiences new to the privacy issue, they can also be used as stand-alones for audiences already familiar with the concepts of privacy and data protection. We encourage you to tailor these materials to meet your own specific needs.

¹Alexander Dix, Built-in Privacy – no panacea but a necessary condition for effective privacy protection. Privacy by Design Issue of Identity in the Information Society Volume 3, Number 2, (August 2010). p 257.

Using this Curriculum

This *Privacy by Design* Curriculum is divided into two modules: the first is conceptual in nature; the second is applied *PbD*.

The first module introduces *Privacy by Design* , and the related concept of *Privacy by ReDesign*.

The second module provides concrete examples of *Privacy by Design* in applied settings, namely:

1. Smart Meters and the Smart Grid
2. Embedding Privacy in Organizational Culture, Policy, and Process
3. Biometric Encryption

We have tried to present these curriculum materials in a way that will make them easy for use by different presenters and their varied audiences. This package includes:

- Presentation slides in PDF format; and
- Detailed instructor resources for each presentation, including links to essential readings, presentation notes, and suggestions for in-depth, further readings.

Our library of resources is constantly expanding. Find the latest at www.privacybydesign.ca.

Course Overview

Module One: The Fundamentals

Presentation 1: *Privacy by Design*: An Introduction

Slide	Title
1.1	What is Privacy?
1.2	Fair Information Practices
1.3	Privacy as a Business Issue
1.4	The Privacy Payoff
1.5	The Perils of Ignoring Privacy
1.6	Market Leaders are Paying Attention!
1.7	<i>Privacy by Design</i>
1.8	Breaking with Tradition: The Zero-Sum Paradigm
1.9	A New Perspective on Privacy
1.10	<i>Privacy by Design</i> : Overview
1.11	Principle One
1.12	Principle Two
1.13	Principle Three
1.14	Principle Four
1.15	Principle Five
1.16	Principle Six
1.17	Principle Seven
1.18	Operationalizing <i>Privacy by Design</i>
1.19	How PIAs Can Help
1.20	The Ultimate Goal

Presentation 2: *Privacy by ReDesign*: Building a Better Legacy

Slide	Title
2.1	The Ideal
2.2	Reality
2.3	Is it Too Late?
2.4	No! Of Course Not!
2.5	<i>Privacy by ReDesign</i>
2.6	What is <i>Privacy by ReDesign</i> ?
2.7	Act Now!
2.8	Identifying <i>PbRD</i> Projects
2.9	Prioritizing: Asking the Right Questions
2.10	Rethink, Redesign, Revive
2.11	Organizing Project Work
2.12	Laying the Foundations for Success
2.13	The Desired End State

Module Two: Applied *Privacy by Design*

Presentation 3: Applied *Privacy by Design*: The Smart Grid

Slide	Title
3.1	The Challenge
3.2	The Smart Grid: What is It?
3.3	Sample Smart Grid: Ontario
3.4	Imagining the Future: Elements of the Smart Grid
3.5	Home, the Most Private of Places
3.6	Key Privacy Risk Areas
3.7	Setting the Standard
3.8	Smart Grid <i>Privacy by Design</i>
3.9	Best Practices
3.10	Simple Application of <i>PbD</i> : Online Customer Information Request
3.11	Advanced Application of <i>PbD</i> : Load Management Program
3.12	The Big Picture: A Privacy Perspective on the Smart Grid
3.13	Benefits of Embedding Privacy at the Design Stage

Presentation 4: Applied *Privacy by ReDesign*: Embedding Privacy in Organizational Culture, Policy, and Process

<i>Slide</i>	<i>Title</i>
4.1	The Privacy Payoff
4.2	Reaping the Rewards
4.3	Time to Re-Invent
4.4	Implement <i>Privacy by Design</i>
4.5	<i>PbD</i> inside the Organization
4.6	The First Step: Put Privacy into the Picture
4.7	Create a Culture of Privacy
4.8	Develop Strong Privacy Policies
4.9	Use Processes
4.10	Leverage Existing Processes
4.11	Example: Adding Privacy into the Risk Management Process
4.12	Privacy Risk Management Maturity Model
4.13	Privacy Risk Management Framework
4.14	Working Through the Process
4.15	Incorporating Privacy into Other Management Processes
4.16	Tools
4.17	The End Result: Privacy Embedded Throughout the Organization
4.18	Reaping the Rewards

Presentation 5: Applied *Privacy by Design*: Biometric Encryption

Slide	Title
5.1	The Context
5.2	Challenges to the Trust Model
5.3	Alternatives to Trust
5.4	Biometrics: A Primer
5.5	Privacy and Security Issues in Biometric Systems
5.6	Traditional Biometrics: A Dead End for Privacy
5.7	Traditional Biometrics: The Bottom Line
5.8	<i>Privacy by Design</i>
5.9	Biometric Encryption
5.10	Biometric Encryption: Process Overview
5.11	Advantages of BE over Traditional Biometrics
5.12	From Theory to Practice: The Ontario Lottery and Gaming Corporation (OLG) Self Exclusion Program
5.13	Privacy- Protective Facial Recognition
5.14	Sample Application of BE
5.15	Facial Recognition using BE
5.16	Lessons Learned: Benefits of Applying <i>PbD</i>