
# Privacy by Design

**Ann Cavoukian, Ph.D.**

Information & Privacy Commissioner
Ontario, Canada

***Privacy by Design*** (*PbD*) was developed by the Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian, back in the‘90s. *Privacy by Design* advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization’s default mode of operation.

The *Privacy by Design* framework employs an approach that is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. *Privacy by Design* 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.

## Global Adoption

In October 2010, regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark Resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection. The resolution, which was co-sponsored by Canadian Privacy Commissioner Jennifer Stoddart and Commissioners from Berlin, New Zealand, the Czech Republic, and Estonia, also:

- Encouraged the adoption of the principles of *Privacy by Design* as part of an organization’s default mode of operation; and
- Invited Data Protection Authorities and Privacy Commissioners to promote *Privacy by Design* by fostering the incorporation of its 7 Foundational Principles in privacy policy and legislation in their respective jurisdictions, and encouraging research into *Privacy by Design*.

This was followed by the U.S. Federal Trade Commission's recognition of *Privacy by Design* in 2012 as one of its three recommended practices for protecting online privacy in its report entitled, *Protecting Consumer Privacy in an Era of Rapid Change* – a major validation of its significance.

More recently, *Privacy by Design* has been incorporated into the European Commission plans to unify data protection within the European Union with a single law – the General Data Protection Regulation. In particular, *Privacy by Design* is reflected in the proposed regulation by requiring data processors as well as producers of IT systems to design their offers in a data-minimizing way, with the most data protection-friendly pre-settings. A strong principle of purpose limitation means that only data necessary for the provision of a service would be processed. The adoption of this regulation should occur in 2014 with the regulation planned to take effect in 2016.

# The 7 Foundational Principles

The 7 Foundational Principles of *Privacy by Design* have proven to be a valuable resource for individuals and organizations around the world. Since the passing of this international resolution, the 7 Foundational Principles of *Privacy by Design* have been translated into 31 official languages.

The objectives of *Privacy by Design* — ensuring privacy protection and gaining personal control over one's own information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the 7 Foundational Principles:

## 1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. *Privacy by Design* 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 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.

## 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

*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.

## 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.

## 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.

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

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

# Trilogy of Applications

*Privacy by Design* provides a method for proactively embedding privacy into information technology, business practices, and networked infrastructures.

## Information Technology

Technology itself is not inherently a threat to privacy. The key lies in how it is used. For example, technology allows us to protect privacy through methods such as severing personal identifiers from data, or by encrypting personal information in a manner such that it can only be viewed by those who are authorized to do so. As technological innovations continue to pose new threats to privacy, Privacy-Enhancing Technologies can minimize these threats.

## Accountable Business Practices

Too often, organizations protest that implementing serious privacy measures increase operating costs while adding nothing to the value of their business. Commissioner Cavoukian has always advocated the idea that privacy is good for business. Her message to both public and private sector organizations: privacy should be treated as a business issue, not a compliance issue. *Privacy by Design* allows businesses to achieve a competitive advantage, by developing and maintaining accountable business practices.

## Physical Design and Networked Infrastructure

When discussing privacy, the physical design of areas where personal information is shared or stored is often overlooked. Think of a pharmacy or hospital waiting room where individuals are often obliged to share personal health information in front of, and within earshot of, others. Similarly, you can have customer records stored safely away in a filing cabinet, but if there are no locks on the filing cabinets, then the privacy of those records cannot be assured. The importance of making sure that an organization's physical assets and infrastructure address privacy requirements cannot be stressed enough.

## Dispelling Myths

Every day it seems that we are assaulted by a new privacy issue – each more sensational than the last. The media appear to have determined that few things are as attention grabbing as a headline describing a new privacy breach or state-sponsored surveillance. Worse, however, is the opportunity these provide for, presumably, well-meaning individuals to speculate on the declining state of privacy in today's society. They advance myths, which unless refuted, are destined to become prophecy.

As privacy professionals, we are all committed to building and preserving a society where personal information is both respected and protected. *Privacy by Design*, of course, is born of the belief that privacy is a cornerstone on which our essential freedoms rest. If we lose our privacy, there will shortly be little to distinguish our nations from totalitarian regimes. While that may sound extreme, it has been borne out in history. And as Benjamin Franklin said, "*Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety*."

The opinions expressed by privacy naysayers often align with three broad overlapping myths:

**Myth 1: "Privacy is dead"**

A wealth of information exists about all of us. New technologies have made it increasingly simple for organizations to collect, analyze, share and search for even the most sensitive personal information. It's too late to reverse the trend, so we should all just get over it.

**Counterpoint**: If privacy is dead, then freedom is dead. And that will never be the case for long, as the human condition is drawn to freedom and liberty. People gravitate to organizations that demonstrate an ability to protect their personal information. Smart organizations will respond with privacy-protective offerings and smarter ways of doing business. In fact, it's not too hard to imagine that privacy will become an element in each company's competitive arsenal. Far from being dead, it is just about to take off!

**Myth 2: "No one cares about privacy anymore"**

Personal information is the substance that makes up our modern identity. Emerging technologies, even as they collect more information about us are also providing greater access to extraordinary new services, conveniences and benefits – not the least of which is the ability to maintain a broad circle of relationships through the latest social media tools. Human beings are social animals and the need to connect is part of the human condition.

**Counterpoint:** Privacy is equally an essential element of the human condition. Our need to preserve private spaces in our lives, to permit reflection, and enjoy moments of solitude and intimacy, is as relevant now as it has ever been. Indeed, it is perhaps more relevant, and increasingly necessary, now that our lives are so networked, inter-connected, and constantly "plugged in." The desire to preserve spheres of privacy will not diminish – it may actually grow.

**Myth 3: "Enhanced security means diminished privacy"**

The privacy debate has been held captive for too long by the win/lose, zero-sum paradigm, which argues that one can have security, but only at the expense of privacy. This argument pits one aim against the other – a false paradigm – claiming that in order to have more of one, you must necessarily give up some of the other.

**Counterpoint:** *Privacy by Design* advances a positive-sum approach to privacy. By following the 7 Foundational Principles of *Privacy by Design*, one is able to conceive of achieving goals well beyond privacy, while also achieving privacy. *Privacy by Design* recognizes the legitimate goals of other stakeholders within the organization in a doubly-enabling, positive-sum manner rather than the either/or, zero-sum model. The "versus" in the equation must be replaced with an "and," enabling multiple results to be achieved, in tandem.

Ultimately, the best rebuttal is an active and well-informed privacy community – one advocating the Principles of *Privacy by Design*.

## *Privacy by Design* Application Areas

Over the past several years, Commissioner Cavoukian has produced more than 60 *Privacy by Design* papers, written with many well-known subject matter experts including business executives, risk managers, legal experts, designers, analysts, software engineers, computer scientists, applications developers in telecommunications, health care, transportation, energy, retail, marketing, and law enforcement.

While some of those papers are "foundational" works, much of the *Privacy by Design* research is directly related to one of nine key application areas:

1. CCTV/Surveillance Cameras in Mass Transit Systems;
2. Biometrics Used in Casinos and Gaming Facilities;
3. Smart Meters and the Smart Grid;
4. Mobile Devices & Communications;
5. Near Field Communications (NFC);
6. RFIDs and Sensor Technologies;
7. Redesigning IP Geolocation Data;
8. Remote Home Health Care;
9. Big Data and Data Analytics.

## Preserving Privacy and Freedom, Well into the Future

We are experiencing an era of near-exponential growth in the creation, dissemination, use and retention of personal information. Whether applied at the level of information technology, business practices, or systems, it is more critical now than ever to embrace *Privacy by Design* if privacy, as we know it, is to survive well into the 21st century.

With increasingly savvy and interconnected users, an organization's approach to privacy may offer precisely the competitive advantage needed to succeed. Privacy is essential to creating an environment that fosters trusting, long-term relationships with existing customers, while attracting opportunity and facilitating the development of new ones. In an ever-changing world of emerging technologies, the right to privacy is more important than ever. We must remain vigilant in the protection of privacy, the bedrock of our freedom and liberty.

Revised: September 2013
Originally Published: January 2009

**Information and Privacy Commissioner of Ontario**
2 Bloor Street East, Suite 1400
Toronto, Ontario • CANADA • M4W 1A8

Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
Web: www.ipc.on.ca • www.privacybydesign.ca
E-mail: info@ipc.on.ca