CERTIFIED
P BY D
RYERSON UNIVERSITY

Privacy by Design
The 7 Foundational Principles

Dr. Ann Cavoukian
Executive Director
Privacy and Big Data Institute

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

In October 2010, regulators at the International Conference of Data Protection Authorities and Privacy Commissioners unanimously passed a Resolution recognizing Privacy by Design as an essential component of fundamental privacy protection. Since then, Privacy by Design has developed a global presence and has been translated into 37 languages.

Privacy by Design advances the view 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. Then, we realized that a more substantial approach is required — extending the use of PETs to a complete Privacy by Design framework. Replacing the existing zero-sum model of either/or with a doubly-enabling positive-sum (win/win) paradigm will be essential.

Privacy by Design extends to a trilogy of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) networked 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 the privacy measures implemented tends to be commensurate with the sensitivity of the data.

The objectives of Privacy by Design — ensuring strong privacy and gaining personal control over one's information, and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the 7 Foundational Principles, which are intended to serve as the foundation of one's privacy practices.

1 Proactive not reactive: preventative not remedial

The Privacy by Design (PbD) framework is characterized by the taking of proactive rather than reactive measures. It anticipates the risks and prevents privacy invasive events before they occur. 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 identify the risks and prevent the harms from arising. 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, as the default. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual in order to protect their privacy — it is already built into the system, by default.

3 Privacy embedded into design

Privacy measures are embedded into the design and architecture of IT systems and business practices. These are not bolted on as add-ons, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is thus 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 the dated, zero-sum (either/or) 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.

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 collected, used, 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. The data subject is made fully aware of the personal data being collected, and for what purpose(s). All the 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 keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. The goal is to ensure user-centred privacy in an increasingly connected world. Keep it user-centric.