Information and Privacy
Commissioner of Ontario

"Privacy by Design"

by

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner
Ontario, Canada

I first developed the term "Privacy by Design" back in the 90s when the notion of embedding privacy into the design of technology was far less popular. At that time, taking a strong regulatory approach was the preferred course of action. Since then, things have changed considerably. This paper summarizes the meaning and origins of *Privacy by Design* — an approach that is now enjoying widespread currency.

What is *Privacy by Design*?

In brief, *Privacy by Design* refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of fair information practices into the design, operation and management of information processing technologies and systems. This approach originally had technology as its primary area of application, but I have since expanded its scope to two other areas. In total, the three areas of application are: (1) technology; (2) business practices; and (3) physical design.

As a broad overarching concept, *Privacy by Design* encompasses many elements in practice:

1. Recognition that privacy interests and concerns must be addressed;
2. Application of basic principles expressing universal spheres of privacy protection;
3. Early mitigation of privacy concerns when developing information technologies and systems, across the entire information life-cycle;
4. Need for qualified privacy leadership and/or professional input; and
5. Adoption and integration of privacy-enhancing technologies (PETs).

IPC Advocacy of *Privacy by Design*

My office has been engaged in promoting all of these elements for many years.

1. Recognizing the benefits of addressing privacy interests and concerns

Privacy by Design begins with the understanding of both the value and benefits of adopting good privacy practices. In the mid-90s, publications by the Office of the Information and Privacy Commissioner of Ontario (IPC) such as *Privacy Protection Makes Good Business Sense* and *Privacy: The Key to Electronic Commerce* argued that all organizations that collect, use and disclose personal information should proactively accommodate the privacy interests and rights of individuals throughout their operations. More than a moral imperative, respecting privacy offered positive-sum dividends to all concerned. The "payoff" to organizations would come in many ways, including: improved customer satisfaction and trust; enhanced reputations; reduced legal liabilities; more efficient operations; commercial gains and enhanced ROI; and, ultimately, enduring competitive advantage.[1] Our mantra, of "Privacy is Good for Business," has been — and continues to be — a central message that we have consistently advocated.

2. Applying universal principles of Fair Information Practices

In order to be effective and credible, building privacy into technologies and operations must be done in a systematic way, with reference to widely-agreed upon privacy principles, standards and other relevant guidance. From the earliest days, the IPC has advocated a principled approach to ensuring *Privacy by Design*. The principles of *Fair Information Practices* (FIPs) give practical expression to individual privacy rights and the obligations of organizations to observe them.

I have always argued that organizations should apply FIPs to their operations. Voluntary international FIPs such as the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, have served as the blueprint for the development of national privacy laws, but in the mid-90s the IPC began to recognize that they also inform the design of information systems. My office has long supported the OECD *Guidelines* and, subsequently, the *CSA Model Code for the Protection of Personal Information* when it was finalized in 1995 to provide "the Canadian context and the new challenges of privacy protection in the information age."[2]

3. Privacy concerns must be identified and mitigated early, and comprehensively

"Build in privacy from the outset" has been my longstanding mantra, to "avoid making costly mistakes later on, requiring expensive retrofits." I have long advocated for the earliest and most iterative identification of privacy issues — preferably at the design stage, but also at the development and implementation stages. Volume II of the 1995 *Privacy-Enhancing Technologies: The Path to Anonymity*, offers a flowchart and discussion of "how the designer can take the user's privacy into account during the different phases of the design process."

Perhaps the clearest expression of my early advocacy for this approach is found in my 1997 paper, *Smart, Optical and Other Advanced Cards: How to do a Privacy Assessment*, which sets out a framework and methodology for building privacy into applications "right from the start." The paper is notable for going beyond specific technologies to insist upon the need to address privacy systematically, at the policy and organizational levels. Privacy Impact Assessment (PIA) tools and similar guidance documents remain a mainstay of my office's output to this very day. Ontario and Canadian governments have emerged as leaders in the development and adoption of PIAs for all projects involving personal information. This year, my office is advancing this further by developing the next generation of tools in this area, focused squarely on not only identifying, but *managing* the risk to privacy. Our PRM, or Privacy Risk Management Tool, will be rolled out later this year.

4. Involving dedicated and qualified leadership and professional input

In our 1995 paper with the Netherlands Data Protection Authority, *Privacy-Enhancing Technologies: The Path to Anonymity*, we coined the term "PETs" and set out a principled approach to building privacy into identity technologies and systems. This was directed squarely at designers of information systems. Applying privacy design practices, features and standards requires increasingly specialized expertise, as information technologies and systems become more complex, and more critical to an organization's operations.

At the same time, knowledge of the organization and of the related privacy sub-domains (legal compliance, technology, business operations, customer relations) are also critical for successful *Privacy by Design* efforts. I have long advocated for dedicated and well-resourced Chief Privacy Officers (CPOs) or similar positions to be created in order to enable strong privacy leadership and accountability.

5. Adoption and integration of privacy-enhancing technologies (PETs)

The growth of computer applications, digitized data and networks into every aspect of our lives has brought novel and profound privacy concerns that cannot be ignored. Fortunately, technology can also help. From a privacy perspective, information and communication technologies (ICTs) are essentially neutral. What matters are the choices we make when designing and using them – ICTs can be privacy-invasive or privacy-enhancing, depending on their design. 'Privacy-enhancing technologies' embody fundamental privacy principles by minimizing personal data use, maximizing data security, and empowering individuals. As mentioned earlier, PETs can be engineered directly into the design of information technologies, architectures and systems by, for example, "minimizing the identity domain" and "minimiz[ing] … personal data stored in a database."[3]

Applied *Privacy by Design*:

By the mid 1990s, the Ontario Government had begun to adopt increasingly sophisticated information and communications technologies and systems, in an effort to benefit from the advantages offered by the emerging "Information Highway."

Of course, the collection, use, sharing and retention of more and more personal information, made possible by large-scale IT projects, posed significant privacy issues.

Given my office's oversight of provincial and municipal government operations, and my presence on privacy and technology issues, my office was increasingly being consulted by public and private sector organizations for advice and guidance on how, exactly, to build in privacy early on — at the design stage of these new systems.

What followed was a succession of joint collaborations on groundbreaking new technology-enabled projects that focused upon developing and applying privacy design principles into the development process so that any privacy-invasive risks could either be minimized or eliminated altogether.

In 1997 we worked with the Smart, Optical and Advanced Card Industry to create a tool designed to help developers of applications using advanced card technologies to understand and implement, in a practical way, the principles of privacy protection.

That same year, we worked with the Ontario Transportation Capital Corporation to design privacy into the newly built electronic toll highway — Hwy 407. The electronic toll surveillance system, used primarily for automatic billing purposes, also resulted in the world's first "anonymous account billing system," as a result of our intervention to address privacy related concerns.

In 1998-99, we developed a paper with the Dutch *Registriekamer*, setting out privacy design criteria for intelligent software agents, *Turning a Privacy Threat into a Privacy Protector*.

Perhaps our largest collaborative *Privacy by Design* project was with the United States Department of Justice, Office of Justice Programs, from 1999-2001. That effort resulted in the release of our *Privacy Design Principles for an Integrated Justice System* in 2000. This paper outlines a set of Privacy Design Principles that would apply to the design and implementation of an integrated justice system, including the criminal justice process, as well as civil court records, juvenile justice information, and probate proceedings. As we noted in the introduction: "This paper is intended to spark informed debate in two areas. The first centers on the Privacy Design Principles and their applicability at various points within the justice system. The second area of debate centers on how technology can be used to implement the design principle policy. In this area, the paper describes 'technology design principles' to help a Technology Design Architect implement the Privacy Design Principles."

All of these elements came together later that year in my presentation, *Privacy By Design: Building Trust into Technology*, to the 1st Annual Privacy and Security Workshop by the Centre for Applied Cryptographic Research (CACR) in 2000.

The Future of Privacy is *Privacy by Design*

Since that time, my office has become ever more deeply involved in helping public and private sector organizations alike understand the importance and need for our *Privacy by Design* approach. We have done this through a long succession of advocacy, guidance, and collaborative initiatives that continues unabated, to this day. Indeed, if anything, it is accelerating!

This need has become ever more important as we enter into a period of accelerating development and adoption of new ICTs and the near-exponential growth in the creation, dissemination, use and retention of personal information. I believe it has become more critical now than ever to embrace the *Privacy by Design* approach. I am gratified that this call is being heard and answered around the world by Privacy and Data Protection Commissioners, technologists, engineers, computer scientists, private and public-sector organizations, privacy advocates, and the public at large. May it grow, well into the future, thereby ensuring the future of privacy.

List of IPC Publications:

Privacy Protection Makes Good Business Sense (October 1994): www.ipc.on.ca/index.asp?layid=86&fid1=327

Privacy-Enhancing Technologies: The Path to Anonymity (August 1995): Volume I: www.ipc.on.ca/index.asp?layid=86&fid1=329

Privacy-Enhancing Technologies: The Path to Anonymity (August 1995): Volume II: www.ipc.on.ca/images/Resources/anoni-v2.pdf

Privacy Protection Models for the Private Sector (Dec 1996): www.ipc.on.ca/index.asp?layid=86&fid1=328

Smart, Optical and Other Advanced Cards: How to do a Privacy Assessment (Sept 1997): www.ipc.on.ca/index.asp?navid=46&fid1=297

Privacy: The Key to Electronic Commerce (April 1998): www.ipc.on.ca/images/Resources/e-comm.pdf

407 Express Toll Route: How You Can Travel the 407 Anonymously (May 1998): www.ipc.on.ca/index.asp?navid=46&fid1=335

Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector (April 1999): www.ipc.on.ca/images/Resources/up-isat.pdf (cf. s.5.6 PETs Design criteria for agents)

Privacy Design Principles for an Integrated Justice System - Working Paper (April. 2000): www.ipc.on.ca/index.asp?layid=86&fid1=318

Privacy Impact Assessment for Justice Information Systems (August 2000): www.ipc.on.ca/index.asp?layid=86&fid1=326

Privacy By Design: Building Trust into Technology. Presentation by Ann Cavoukian, Ph.D. to the 1st Annual Privacy and Security Workshop. Centre for Applied Cryptographic Research (CACR), Toronto, Ontario, Canada - November 10, 2000: www.cacr.math.uwaterloo.ca/conferences/2000/isw-sixth/cavoukian.ppt

Endnotes

1 For a more thorough exposition of this payoff, see Ann Cavoukian & Tyler Hamilton, *The Privacy Payoff: How Successful Businesses Build Customer Trust*, McGraw-Hill (2005).

2 *Privacy Protection Models for the Private Sector* (Dec 1996): www.ipc.on.ca/index.asp?layid=86&fid1=328.

3 *Privacy-Enhancing Technologies: The Path to Anonymity* (August 1995) Volume II: www.ipc.on.ca/images/Resources/anoni-v2.pdf.

Published: January 2009

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

Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Email: info@ipc.on.ca