Privacy by Design

Ann Cavoukian, Ph.D.

Information & 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 (FIPs) into the design, operation and management of information processing technologies and systems. This approach originally had information 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) information technology; (2) business practices; and (3) physical design and infrastructures.

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

1. Recognition that privacy interests and concerns must be addressed proactively;
2. Application of core principles expressing universal spheres of privacy protection;
3. Early mitigation of privacy concerns when developing information technologies and systems, throughout the entire information life cycle —end to end;
4. Need for qualified privacy leadership and/or professional input;
5. Adoption and integration of privacy-enhancing *technologies* (PETs);
6. Embedding privacy in a positive-sum (not zero-sum) manner so as to enhance both privacy and system functionality; and
7. Respect for users’ privacy.

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* 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 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.

Ontario and Canadian governments have emerged as leaders in the development and adoption of PIAs for all projects involving personal information.

[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

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, we can enlist the support of technology to come to the aid of privacy. 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]

6. Embedding Privacy in a Positive-Sum Way

Adding privacy to information technologies and systems should not require substracting security, usabiliy, efficiency, organizational control or other desirable functions or attributes. The belief that privacy is necessarily opposed to other goals, requiring trade-offs, is false — it is a false dichotomy. Rather, the hallmark of applied *Privacy by Design* is overcoming this prevailing zero-sum mentality and paradigm to achieve positive-sum, "win-win" results. Indeed, when applied to privacy-invasive technologies, the *Privacy by Design* approach can be transformative in nature.

7. Respect for Users' Privacy

This where it all begins.This is where it ends.

Applied *Privacy by Design*

By the mid 1990s, the Ontario Government had begun to adopt increasingly sophisticated information and communications technologies, 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 both 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.

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

What followed was a succession of joint collaborations on groundbreaking new technology-enabled projects that focused on 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 — Highway 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 to 2001. That effort resulted in the release of our *Privacy Design Principles for an Integrated Justice System* in 2000 (and subsequent PIA). 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 *Privacy by Design: Building Trust into Technology*, my presentation to the 1st Annual Privacy and Security Workshop by the Centre for Applied Cryptographic Research (CACR), the first of a series on Privacy by Design..

Privacy by Design in the 21st Century, and Beyond

Since that time, my office has become ever more deeply involved in helping public and private sector organizations 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! As our work since 2000 (below) illustrates, the PbD concept can be applied at many levels, from specific technologies, to organizational practices, extending to entire information ecosystems and architectures.

PbD Applied to Information Technologies

PbD originated from the concept of PETs, and so a focus on technologies remains a source of inspiration for us when advocating building in privacy from the outset.

In May 2002 we developed a schema for doing just that, called *7 Essential Steps for Designing Privacy into Technology*. This schema was a byproduct of a larger ongoing international project to define, evaluate and independently certify PETs.

In 2004, I began to advocate designing privacy into security technologies in a way that could achieve both, thereby overcoming zero-sum paradigms. My publication *Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift* identified opportunities to apply the *Privacy by Design* approach to emerging security technologies, for example, whole body imaging.

We partnered with IBM in 2004 to model a privacy markup language ("Extensible Privacy Assertion Language" or EPAL) that could express the statutory requirements of Ontario's privacy and access to information law in a way that could be applied automatically by computers. A similar standard for machine-to-machine privacy negotiations was also examined in 2000 (P3P).

Technologies that can invade — or protect — our privacy in new ways have often been the focus of our *Privacy by Design* advocacy efforts. This has been especially true of biometrics and radio frequency identification (RFID) technologies — identification, surveillance and control technologies which, nevertheless, can be designed and used with effective privacy controls built in. We have issued numerous guidelines on both technologies over the years.

Certain kinds of privacy technologies are easy to promote, because the benefits of using them outweigh the costs. Additionally, requirements such as mandatory breach notification provide strong incentives to adopt *Privacy by Design* technologies! Thanks to breach notification requirements and my office's oversight powers, personal health information in Ontario must be encrypted whenever it leaves the custodian's control. My office has issued guidance on use of data encryption, access control and audit technologies.

Lately, I have been particularly enthusiastic about a class of PETs that I call *PETs Plus*, or *transformative technologies*, because they apply *Privacy by Design* principles so well and so thoroughly that they actually transform privacy-invasive technologies into privacy-protective ones. Examples include Secure Visual Object Encoding, capable of real-time obfuscation of identities in public CCTV footage — until needed for evidence by law enforcement. Another is Biometric Encryption, a technology capable of putting individuals in exclusive control of their own biometric identifiers, with no universal template that could otherwise be matched to templates contained in other databases.

We sometimes encourage privacy innovation by issuing a challenge. This has been true of my latest efforts to add an on/off device for Ontario citizens to control transmission of unique identifying data embedded in the new Enhanced Driver's Licences. We have been delighted with the response to date, and are particularly enthused about applying the concept to RFID-based access and payment cards.

Sometimes the technology doesn't yet exist or is not well-understood. Still, we can imagine how *Privacy by Design* principles would apply, say, to screening or predictive systems, or to Intelligent Software Agents.

PbD Applied to Organization Practices

While we often focus on specific technologies (the more user-centric the better) to illustrate *Privacy by Design* concepts, in practice it is usually the organization that is the most effective focus of *PbD* efforts, especially where compliance with privacy laws is required. Many organizations, be they public or private collect, use and disclose a considerable amount of personally-identifiable information (PII) in the course of doing business. The responsible and effective management of that PII requires a broader, more thorough *PbD* approach.

It has become a critical necessity in today's data-rich, networked world to ensure an organization's operations embody privacy that has been designed-in early, as well as holistically and effectively. Applying the *Privacy by Design* approach to operations in a proactive way is good for privacy, good for consumers' confidence and trust, and therefore, good for business.

In August 2001 my office released the *Privacy Diagnostic Tool (PDT) Workbook*, a practical hands-on tool to help organizations systematically apply Privacy by Design across their entire enterprise. The PDT Workbook remains our most popular downloaded publication.

We followed up in November 2003 with our guidance publication *Privacy and Boards of Directors: What You Don't Know Can Hurt You* (updated July 2007) which argued that privacy protection starts at the top and must be have a C-suite presence to provide real and effective organizational accountability.

Working with industry associations over the years, we continue to advance our *Privacy by Design* best practices approach to all association members in our joint guidance publications, such as *Incorporating Privacy into*

Marketing and Customer Relationship Management (May 2004), *Contactless Smart Card Applications: Design Tool and Privacy Impact Assessment* (April 2007), and *RFID and Privacy: Guidance for Health-Care Providers* (January 2008).

In June 2005, following the coming into force of Ontario's Health Information Privacy law, we issued *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act* (2005), a comprehensive tool for health information custodians to ensure privacy protections are built into their operations and processes.

More exciting *PbD* work is on its way. My office is developing the next generation of guidance tools for public and private sector organizations, focused squarely on not only identifying, but managing the risk(s) to privacy. Our work on Privacy Risk Management will be rolled out later in 2009.

PbD Applied to Information Architectures

In recent years, I have been turning my attention more and more to the broad information ecosystems in which both technologies and organizations are embedded and must function. I ask the question: How can proactive *Privacy by Design* principles be applied to information architectures and interoperable networks?

To begin, we need common privacy reference points and standards. To this end, I chaired a Working Group of the international Privacy and Data Protection Commissioners in 2005-2006 to harmonize the various privacy codes and practices currently in use around the world. The result was the creation of a single harmonized instrument, the *Global Privacy Standard*, which for the first time identified data minimization explicitly as a universal privacy principle.

In 2005, I published a research paper, *Privacy and the Open Networked Enterprise*, that set out five major privacy challenges facing all organizations as they adapt their business models to an increasingly data-rich, networked world. The privacy solutions are complex, involving in most instances a careful mix of technology, policy/operational and extra-organizational adjustments. Privacy and the O.N.E. stands as a useful map to guide further research into – and application of – our *Privacy by Design* approach.

The same year, I began exploring identity-related privacy issues in greater depth. I recognized that privacy was at risk in a networked world of interoperable digital identifiers, and that more transparency and user-centricity had to be baked into the emerging identity management layer of the internet. It was necessary to reach the technical architects who were responsible for building this layer. Inspired by the "7 Laws of Identity" (a.k.a. "technologically-necessary principles of identity management") formulated on an open blog by a global community of experts through the leadership of Kim Cameron, Chief Identity Architect at Microsoft, I published an annotated commentary. *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age* (Oct 2006) that advocated embedding privacy early into interoperable identity management systems and technologies. The 7 Laws of Identity offer strong potential for computer users to combat online fraud, minimize disclosure of their personal information, and assume greater control over their privacy when online. The result is a positive-sum, win-win situation for both consumers and e-commerce.

With the advent of cloud computing, I recognized that more and more personal data transactions are taking place "in the Cloud" with little knowledge or direct involvement of individuals. I asked: what happens to personal identity data when individuals aren't even sitting behind their computers anymore? How can privacy be designed into the Cloud Computing paradigm — understood as a vast, interconnected, virtual supercomputing platform available from anywhere, any time? Answered in my May 2008 paper, *Privacy in the Clouds: Privacy and Digital Identity - Implications for the Internet*, I explored possible technological solutions to ensure that individuals will be able to exercise informational self-determination, or data privacy, in an era of networked grid computing, exponential data creation, ubiquitous surveillance and rampant online fraud. The paper describes typical "Web 2.0" use scenarios, suggests a number of technology building blocks for protecting and promoting privacy online, and concludes with a call to develop a privacy-respectful information technology ecosystem for identity management.

In January 2009, I released *The New Federated Privacy Impact Assessment (F-PIA) Building Privacy and Trust-enabled Federation*, an assessment tool intended for use by companies that will be sharing their online identity management systems. This discussion paper outlines an approach to enhancing privacy and trust in a federated identity system and serves as a practical guide for organizations to achieve a robust end-to-end information ecosystem where both consumer and supplier are the beneficiaries in a win-win scenario.

The Future of Privacy Lies in *Privacy by Design*

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, I believe it is more critical now than ever to embrace the *Privacy by Design* approach if privacy, as we know it, is to survive well into the 21st century.

In a world of 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.

On January 28, 2009 — International Data Privacy Day — I hosted the inaugural *Privacy by Design Challenge* with the Toronto Board of Trade. Among the speakers were executives from the world's major companies such as Intel, IBM, Microsoft, HP, Sun Microsystems and Facebook, as well as emerging companies such as Peratech and Privacy Analytics, each showcasing their innovative privacy technologies. Our Privacy by Design Challenge event was a sold-out success, and will be held every year on Data Privacy Day, featuring a competition and award for best privacy design.

I am gratified that this call is being heard and answered around the world by Privacy and Data Protection Commissioners, technologists, business leaders, politicians, privacy advocates, and the public at large. May it grow, well into the future, thereby ensuring the continued presence of privacy and liberty.

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

7 Essential Steps for Designing Privacy into Technology (May 2002)
www.ipc.on.ca/english/Resources/Best-Practices/Best-Practices-Summary/?id=294

Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift (June 2004)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=245

EPAL Translation of the Freedom of Information and Protection of Privacy Act (March 2004)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=344

Video: A Word About RFIDs and Your Privacy in the Retail Sector (March 2006)
www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=663

Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines) (June 2006)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=432

Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy (March 2007)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=608

Encrypting Personal Health Information on Mobile Devices (May 2007)
www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=613

Wireless Communication Technologies: Safeguarding Privacy & Security (Aug 2007)
www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=645

RFID and Privacy: Guidance for Health-Care Providers (January 2008)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=724

How to Preserve Freedom and Liberty: Design Intelligent Agents to be Smart and Respectful of Privacy (August 2008)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=784

Fingerprint Biometrics: Address Privacy Before Deployment (November 2008)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=816

Transformative Technologies Deliver Both Security & Privacy: Think Positive-Sum not Zero-Sum (Jul 2008)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=758

Privacy & Radical Pragmatism: Change the Paradigm (August 2008)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=788

Moving Forward from PETs to PETs Plus: The Time for Change is Now (January 2009)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=834

Adding an On/Off Device to Activate the RFID in Enhanced Driver's Licences: Pioneering a Made-in-Ontario Transformative Technology that Delivers Both Privacy and Security (March 2009)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=854

Privacy Diagnostic Tool (PDT) Workbook (August 2001)
www.ipc.on.ca/english/Resources/Best-Practices/Best-Practices-Summary/?id=293

Privacy and Boards of Directors: What You Don't Know Can Hurt You (Nov 2003, updated July 2007)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=240

Incorporating Privacy into Marketing and Customer Relationship Management (May 2004)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=234

Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act (June 2005):
www.ipc.on.ca/english/Resources/Best-Practices/Best-Practices-Summary/?id=574

Contactless Smart Card Applications: Design Tool and Privacy Impact Assessment (May 2007)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=614

Creation of a Global Privacy Standard (Nov 2006)
www.ipc.on.ca/english/Resources/Best-Practices/Best-Practices-Summary/?id=575

Privacy and the Open Networked Enterprise (June 2005)
http://www.ipc.on.ca/images/Resources/opennetw.pdf

7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age (Oct 2006)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=470

Privacy in the Clouds: Privacy and Digital Identity - Implications for the Internet (May 2008)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=748

The New Federated Privacy Impact Assessment (F-PIA) Building Privacy and Trust-enabled Federation (March 2009)
www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=836

***Privacy by Design* website: www.privacybydesign.ca**

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