Patience, Persistence, and Faith: Evolving the Gold Standard in Privacy and Data Protection

Ann Cavoukian

Patience, Persistence, and Faith

Evolving the Gold Standard in Privacy and Data Protection: Chronicles of a "Crusader"

Ann Cavoukian

Information and Privacy Commissioner, Ontario

Abstract. *Privacy by Design* (*PbD*) is a concept that was developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, in the '90s. It prescribes that privacy be embedded directly into the design and operation, not only of various technologies, but also of business processes and networked infrastructure. Instead of treating privacy as an after-thought – "bolting it on after the fact" – *PbD* is proactive and preventative in nature.

Through years of advocacy and encouragement, PbD is now being widely adopted globally by a growing number of organizations and jurisdictions. This paper outlines the foundations of PbD, and traces its evolution from a conceptual framework into a practical one that has been recognized internationally as the gold standard in privacy and data protection.

Personal information, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational, is the substance that makes up our modern identity. Our digital footprints and shadows are being gathered together, bit by bit, megabyte by megabyte, terabyte by terabyte, into personas and profiles and avatars – virtual representations of ourselves that exist in thousands of simultaneous locations. These technologies give us access to extraordinary new services, conveniences, efficiencies and benefits, undreamt of by our parents. At the same time, novel risks and unimagined threats are emerging from this digital cornucopia. Identity fraud and theft are the diseases of the Information Age, along with new forms of deception and social engineering made possible by the surfeit of data.

These developments have prompted some critics to pronounce that privacy is either dead or dying[1]. I don't believe that to be the case, but there is no question that our fundamental ideas about identity and privacy, the strategies that we have collectively pursued, and the technologies that we have adopted, must evolve and adapt to keep

[1] See, for example, Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century. O'Reilly Media, California (2000); Robert O'Harrow, No Place to Hide: Behind the Scenes of our Emerging Surveillance Society. Free Press, New York (2005); David Brin, The Transparent Society. Addison-Wesley, New York (1998); and Jerry Rosenberg, The Death of Privacy. Random House, New York (1969).

apace with our rapidly changing world of connectivity, networking, participation, sharing, and collaboration.

At stake is not only our privacy, but also the consumer confidence and trust that underpins and enables today's information society. What will privacy mean, and how will privacy survive, and hopefully thrive, as a viable human right, operational value, and critical enabling trust factor, in a world where the individual is increasingly removed from personal involvement in data-rich transactions? What will informational self-determination – the basis of current privacy laws and practices – mean when data is increasingly stored and processed away from personal computing devices, in the world of a nebulous "Cloud?"

These are precisely the kinds of questions I have been grappling with in my 20 year career in privacy. My attempts to answer these questions – to imagine a future where privacy continues to exist in some form we find recognizable – are the foundations of the work for which I am honoured to have received the Kristian Beckman Award. *Privacy by Design* – the concept I pioneered relating to engineering privacy directly into the design of new technologies, accountable business practices, and networked infrastructure as a core functionality – is an approach I have advocated for many years. It has, only recently, reached a tipping point, and now appears to be gathering momentum around the world.

This paper traces the roots of the concept, and chronicles some of the highlights in my ongoing crusade to see *Privacy by Design* implemented with sufficient breadth and depth that it effectives assures a future for privacy and all the social values it enables.

Privacy Will Always Matter

Privacy is not dead, and will never die, given the essential role it plays in preserving our freedoms, but it is, perhaps, beleaguered. Practical obscurity – the basis for privacy norms throughout much of history – is fast disappearing. The functional impediments to surveillance that once protected privacy, by default – such as data processing and storage costs, and the difficulty of linking files from multiple databases – are increasingly irrelevant.

Privacy, famously described by American Justices Samuel Warren and Louis Brandeis as "the right to be let alone,"[2] is closely related to individual dignity and integrity, personal autonomy, freedom of association, and independence. It is the underpinning of many of the rights and values we hold dear, and has long been – and still remains – a vital component of free and democratic societies. Historically, when a society devolves from a free and democratic one into a totalitarian state, privacy is the first thread to unravel.

[2] Warren, S. and Brandeis, L.: *The Right to Privacy*. Harvard Law Review 4, 193-220 (1890)

Our need to preserve private spaces in our lives, to permit intimacy, and to enjoy solitude, is as relevant now as it has ever been. Indeed, it is perhaps *more* relevant now that our lives are so networked, inter-connected, and "plugged in."

The idea that privacy is under attack is not new, but the weapons of choice have changed over time. Over hundreds of years, critics have raised concerns about the privacy implications of almost every new technology, from the camera to the telephone to the personal computer. And those who have taken it upon themselves to protect our privacy have been forced to innovate similarly, developing new strategies and expanding their arsenals as new threats emerge.

One Giant Leap: The Story of PETs

If privacy is gasping for air, it is most certainly, at least in part, because traditional ways of preserving privacy are no longer sufficient or relevant. This has been the case for quite some time.

But in the 1990's, the seeds of a way forward were planted when it began to become clear that our dated approach to protecting privacy, which was based on the assumption that privacy and technology were necessarily opposed to one other, had no viable future. The forward march of technology could not – and arguably should not – be stopped. Somehow, privacy had to find a way to live on.

This led to the development of Privacy-Enhancing Technologies (PETs), which are predicated on the idea of enlisting the support of technology to *enhance* privacy, rather than *encroach* upon it. Believe it or not, the idea was a radical one at the time.

PETs are information and communications technologies that strengthen the protection of personal privacy in an information system by preventing the unnecessary or unlawful collection, use, and disclosure of personal data, or by offering tools to enhance an individual's control over his/her personal data.

The concept grew, in part, out of feeling that encryption technologies could help individuals and organizations protect personal information in the face of the widespread dissemination of personal computers and the advent of the Internet as a (then) new medium of communications. Western governments, however, were trying to restrict the use and export of encryption products, and engineer surveillance "backdoors" into the emerging digital telecommunications infrastructures. This met with fierce resistance from cryptographers, privacy advocates, rights groups, and business interests. If new information and communications technologies threatened to invade individual privacy, the thinking went, then these types of privacy-enhancing technologies, that could empower individuals and restore trust, were the solution.

We first advanced the concept of "PETs" in a collaborative work between my office and the Netherlands Data Protection Authority in 1995.[3] From the outset, PETs emphasized the need to incorporate the universal principles of Fair Information Practices (FIPs) – universal privacy principles for handling personal data –into the actual code and operation of information processing technologies and systems.

First codified by the OECD in 1980, there are many articulations of Fair Information Practices, including the E.U. Directive on Data Protection, Canada's CSA Privacy Code, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, the U.S. Safe Harbor Principles, and the harmonized Global Privacy Standard.[4] Despite minor differences in language and emphasis, these FIPs all reflect the following fundamental concepts:

- **Purpose Specification and Use Limitation** – reasons for the collection, use, disclosure and retention of personally identifiable information should be identified at or before the time of collection. Personal information should not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law;
- **User participation** – individuals should be empowered to play a participatory role and exercise controls during the life cycle of their own personal data;
- **Strong security** – the confidentiality, integrity and availability of personal data should be safeguarded, as appropriate to the sensitivity of the information; and

In their design and implementation, PETs should ideally promote *all* of these meta-principles. The use of strong encryption technologies to secure detailed customer records against unauthorized access, for example, is extremely valuable, but it speaks little to data minimization and user participation. Building in privacy principles early and comprehensively into information technologies and systems is central to good PETs and would later, through a process of incremental refinement, become the anchor for my trademark *Privacy by Design* approach.

Traditional PETs contribute to the achievement of the privacy ideal of informational self-determination – the *individual's* ability to exercise a measure of control over the collection, use and disclosure of their personal information. They have typically been defined as performing the following functions:

- preventing unauthorized access to personal communications and stored files;

---

[3] Information and Privacy Commissioner/Ontario, Registratiekamer/The Netherlands: Privacy-Enhancing Technologies: The Path to Anonymity (Volume I). (1995) http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329

[4] Information and Privacy Commissioner/Ontario, Creation of a Global Privacy Standard. (2006): www.ipc.on.ca/images/Resources/gps.pdf

- automating the retrieval of information about data collectors' privacy practices and automating users' decision-making on the basis of these practices;
- preventing automated data capture through cookies, HTTP headers, web bugs, spyware, etc.;
- preventing communications from being linked to a specific individual;
- facilitating transactions that reveal minimal personal information; and
- filtering unwanted messages.

As PETs are user-centric tools and functions, this list has not been significantly lengthened in over a decade. Over time, we began to wonder whether we had perhaps placed unnecessary boundaries around PETs. Were they cryptographic primitives, software or hardware applications, components embedded in larger systems, or entire information systems? Should PETs be understood to include only technologies under the exclusive control of the individual, or was there room for a more expansive definition that included important and complementary infrastructure components beyond the control of the individual?

PETs Plus: Putting a Positive Spin on Privacy

Within 10 years of the concept of PETs being clearly articulated, the "new normal" of surveillance – deeper and broader than ever before – was such that the limitations of PETs were becoming clear. The door to a more expansive understanding had to be opened.

PETs embody fundamental privacy principles by minimizing personal data use, maximizing data security, and empowering individuals. They are useful, but no longer sufficient in and of themselves to assure sustained, meaningful privacy protection. And while FIPs remained relevant, a significant challenge was that the early drafters and adopters of FIPs clearly had in mind large mainframe computers and centralized electronic databases. They could never have imagined how leapfrogging revolutions in sensors, bandwidth, storage, and processing power would converge into our current hyper-connected Web 2.0 world of ubiquitous data availability.

A second challenge with the PETs approach was that it kept the privacy conversation contained to a relatively small suite of technologies, and therefore marginalized. Further, organizations were inclined to think that they could have technology systems that *either* protected privacy *or* were effective in meeting their business objectives – not both. The kinds of arguments that were being made in support of PETs did little to disabuse them of this notion.

As surveillance technologies continued to expand throughout the 1990's, I observed that privacy was constantly losing out in debates that pitted it against values like public safety, security, and even efficiency. Some of the surveillance control

technologies that privacy was losing out to at the time included (typical objectives shown in brackets):

- Public and private video surveillance (public safety)
- Employee monitoring and surveillance (corporate data security)
- Network monitoring, profiling and database analytics (network forensics, marketing)
- Device location tracking (safety, resource allocation, marketing)
- "Whole of customer" transaction aggregation (customer service)
- Creation and uses of "enriched" profiles to identify, verify and evaluate (security)
- Creation and uses of interoperable biometric databases (access control/security)

These types of surveillance systems were being built around the basic assumption that users/subjects had to give up some of their privacy in order to benefit from improved system security and functionalities. This is how privacy was being increasingly "trumped" by social, legal, and economic imperatives: it was being characterized as a zero-sum tradeoff – always coming at the expense of other interests against which it had to be "balanced."

But balance metaphors assume that the two interests being balanced are always in conflict, and that an increase in one necessarily translates into a decrease in the other. More privacy equals less security; more security equals less privacy.[5] This simply isn't the case.[6]

Ultimately, PETs were effective in some situations, but less so in others, and their long-term strategic value to advancing the cause of privacy into the mainstream appeared to be limited. In my view, PETs *Plus* – Privacy-Enhancing Technologies applied in the context of a positive-sum, not zero-sum paradigm – represented the next evolution of PETs.

By adding a "positive-sum" outlook to the design and use of information and communication technologies, PETs *Plus* made it possible to conceive of achieving goals *beyond* privacy, while *also* achieving privacy goals. It recognized the legitimate goals of other participants or stakeholders in the development process, such as, for example, those of the system owner and operator, in a positive-sum rather than zero-sum, "either/or" model. Thus the functional and operational objectives of a

[5] See Julian Sanchez's excellent blog posting (February 4, 2011) on the shortcomings of balance metaphors at www.juliansanchez.com, which is based on Orin Kerr's An Equilibrium-Adjustment Theory of the Fourth Amendment. Harvard Law Review, Vol. 125 (forthcoming) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1748222.

[6] Indeed, the balance metaphor is coming under growing criticism. See, for example, Daniel Solove: Nothing to Hide: The False Tradeoff Between Privacy and Security. Yale University Press (forthcoming, 2011).

system (e.g., to transport and route electronic communications, to process a payment, or provide a service), and other security, surveillance, and anti-fraud detection goals, could be achieved while *also* protecting privacy. It was a conceptual shift that would, over time, prove critical in engaging organizations meaningfully in the privacy issue. The time had come to move beyond false dichotomies and short-sighted "balancing acts."

Beyond Individual Responsibility

Throughout this period, changes in information technology were making it increasingly difficult for individuals to exert meaningful control over the collection, use, and disclosure of their personal information. Significantly, at about the same time, organizations were beginning to face pressure to provide better privacy assurances, for a number of reasons.[7]

By the mid-'90s, there was considerable public discussion in the European Union, Canada and the United States about the merits of good privacy practices flowing from the anticipated coming into force of the European Data Protection Directive.[8] The EU Directive sought to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data. Significantly, when transposed to EU Member national law, the EU Directive would require foreign jurisdictions and businesses to meet its "adequacy" requirements in order to receive transfers of any personal information about EU citizens.

In Canada, a broad coalition of business and consumer interests was meeting to establish a national, voluntary privacy code to guide the legitimate information requirements of business, industry and institutions operating in the information age. Their efforts would ultimately be legislated in the *Personal Information Protection and Electronic Documents Act* (PIPEDA). In the United States, negotiations began with the EU on a "Safe Harbor" framework agreement to establish similar ground rules for the processing of personal information by U.S. businesses.

Aside from these regulatory developments, growing interest in electronic commerce was also putting a new spotlight on privacy. The fulfillment of the promise of the Information Age would rely, in large measure, on the ability to foster the confidence and trust necessary for active consumer participation. Against this background, my office published several white papers such as, *Privacy Protection*

---

[7] In 1995, Don Tapscott and I co-authored Who Knows: Safeguarding your Privacy in a Networked World. Random House, Toronto (1995) that captures the spirit of this time.

[8] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 of 23.11. (1995)

Makes Good Business Sense,[9] and *Privacy: The Key to Electronic Commerce*[10] that argued that any organization that collects, uses and/or discloses personal information should proactively accommodate the privacy interests and rights of individuals, throughout its operations. More than a moral imperative, respecting privacy would offer a business "payoff" to organizations in the form of: improved customer satisfaction and trust; enhanced reputations; reduced legal liabilities; more efficient operations; commercial gains and enhanced ROI; and, ultimately, an enduring competitive advantage.

Toward a New Paradigm: *Privacy by Design*

Against this backdrop, the Ontario Government, like many other public and private sector organizations, had, since the mid 1990's, begun to adopt increasingly sophisticated information and communications technologies in an effort to leverage the benefits of the emerging "Information Highway," as it was then called. Of course, the collection, use, sharing and retention of more and more personal information, made possible by these large-scale IT projects, posed significant privacy issues.

Given my office's role in overseeing provincial and municipal government compliance with access to information and privacy laws, and my position on privacy and technology issues, I was increasingly being consulted by the government, as well as other public and private sector organizations, for advice and guidance on how, exactly, to proceed. The answer involved being proactive and building privacy in *early on* — at the design stage of these new systems, namely, *Privacy by Design*.

What followed was a succession of joint collaborations[11] on groundbreaking new technology-enabled projects that focused on developing and applying Privacy by Design principles into the development process so that any privacy-invasive risks could either be minimized or eliminated altogether.

---

[9] Information and Privacy Commissioner/Ontario, Privacy Protection Makes Good Business Sense, www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=327

[10] Information and Privacy Commissioner/Ontario, Privacy: The Key to Electronic Commerce, www.ipc.on.ca/images/Resources/e-comm.pdf

[11] See, for example, Information and Privacy Commissioner/Ontario publications: Smart, Optical and Other Advanced Cards: How to do a Privacy Assessment, www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=297; 407 Express Toll Route: How You Can Travel the 407 Anonymously, www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=335; Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector, www.ipc.on.ca/images/Resources/up-isat.pdf; Privacy Design Principles for an Integrated Justice System - Working Paper, www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=318

All of these elements came together 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.[12]

At the same time, market changes, technological developments, and evolutions within the privacy community converged such that by 2000, when the deeply influential Computers, Freedom and Privacy (CFP) conference held its 10th annual meeting in Toronto, organizers and participants set aside – for the first time – their traditional focus on legislative privacy protections.

In an exploratory *Workshop on Freedom and Privacy by Design*, participants considered how technology could be leveraged to bring about strong protections of civil liberties that would be guaranteed by the technologies themselves.[13] The workshop aimed at developing principles for designing and implementing information architectures, strategies and evaluation criteria that could be inherently privacy protective. To do so, it brought together programmers, cryptographers, and systems architects with lawyers, social scientists, writers and user/experts.

Still, their focus remained largely technological. By contrast, my office's work on *Privacy by Design*, though rooted in PETs, recognized the need to embed privacy at the design stages of information technologies, architectures, *and* systems. By applying 7 foundational principles, the objectives of *Privacy by Design* could be met in all of these areas.

The 7 Foundational Principles of *Privacy by Design*

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy – Keep it User-Centric

These principles are applied within the context of data minimization – the idea that the collection, use, disclosure and retention of personal information should be

[12] Presentation by Ann Cavoukian, Ph.D. to the 1st Annual Privacy and Security Conference, Centre for Applied Research, *Privacy by Design: Building Trust into Technology* www.cacr.math.uwaterloo.ca/conferences/2000/isw-sixth/cavoukian.ppt

[13] Computers, Freedom and Privacy workshop proceedings, www.cfp2000.org/workshop/materials/

minimized wherever, and to the fullest extent, possible. This concept, which had been missing from most articulations of Fair Information Practices, appeared in the Global Privacy Standard that was developed by a Working Group of Commissioners that I chaired, and that had as its sole focus the creation of an internationally harmonized set of FIPs.[14]

My broader, more holistic approach to protecting privacy, by design, would begin to take hold in the first decade of the new millennium. *Privacy by Design* would also begin to move the privacy debate out of the win/lose, zero-sum paradigm. As a result, it would challenge organizations to think creatively about how all system objectives – including privacy – could be met. This opened the door for actively bringing privacy into the development process – a substantial break with traditional approaches that often left privacy to the last minute or later (to the extent that it was addressed at all), placing the bulk of the responsibility in the hands of individual consumers.

Privacy by Design **in the Post-9/11 World: Challenges and Opportunities**

In the meantime, the events and consequences of September 11, 2001 challenged assumptions among many privacy advocates, freedom fighters and technologists that individual privacy was necessarily paramount to all other interests in society. They found it increasingly difficult to defend privacy interests in an atmosphere characterized by visceral public fear and a collective desire for security.

Almost overnight, the privacy threat model changed. Governments enacted legislation and put in place initiatives that trumped traditional information privacy legislation and individual rights, often enlisting private-sector organizations to collect and use more granular personal information than ever before.

This was the classic zero-sum paradigm writ large: the more we have of one interest (public security), the less we can have of another (individual privacy). Privacy could never win out – and arguably could not even survive – within this zero-sum framework.

Unpopularly at first, I challenged the underlying premise that privacy necessarily had to be ceded in order to gain security benefits, arguing that both could be achieved at the same time. I posited that many security technologies could be redesigned to remain effective, while minimizing or eliminating their privacy invasive features. By substituting a new premise - that privacy and security were two complementary sides of an indivisible whole (not opposites), I argued that we could design technologies that protect public safety *without* sacrificing privacy. What a concept!

My approach during this period was three-pronged:

---

[14] Information and Privacy Commissioner/Ontario, Creation of a Global Privacy Standard. (2006), www.ipc.on.ca/images/Resources/gps.pdf

1. Challenging the privacy community to question existing paradigm assumptions, and to raise the level of debate on security and privacy above traditional, simplistic, either/or viewpoints.
2. Challenging two distinct groups: 1) legislators, policy analysts and legal counsel that draft legislation focused on security and public safety, and 2) directors, managers, individuals, who develop Requests for Proposals (RFPs) and set the procurement 'specs' for security technologies, to be more mindful of how privacy interests could be accommodated in their work.
3. Challenging solution providers – engineers, technologists, software designers, and other developers of technology and their industry associations - to introduce privacy concepts into the policy statements of their organizations and associations, and, more importantly, to embed privacy directly into the concept, design and implementation of their technology solutions. Namely, add privacy features into code, making it a core functionality.

Over time, this view gained credence, and privacy principles began to be introduced into otherwise security-focused frameworks.

The Privacy Payoff: Taking *Privacy by Design* into the Business Community

While the security community remained an essential focus in the aftermath of September 11, it was clear to me that, in order to ensure meaningful privacy protection well into the future, I had to continue my work to entrench privacy as a basic business practice. So, during the early 2000's, I redoubled my efforts to engage the business community.

My arguments were published in 2002 as *The Privacy Payoff*,[15] a book I co-authored with Tyler Hamilton. The premise was simple: businesses were collecting information about their customers through knowledge-based technology, hoping to better serve their customers and, in turn, increase their profits. But most were overlooking one key point – customers didn't like how they went about this.

Going beyond quick fixes, *The Privacy Payoff* offered companies concrete steps to avoid the risks of the privacy minefield and reap the advantages of a privacy-sensitive corporation. It discussed global regulations and trends, drafting and implementing a privacy policy, and more. The central message – that adopting good privacy and security practices paid back multiple dividends and was highly desirable, regardless of legal and regulatory requirements – remains to this day a core axiom of the *Privacy by Design* approach.

[15] Ann Cavoukian & Tyler Hamilton, The Privacy Payoff: How Successful Businesses Build Customer Trust. McGraw-Hill Ryerson (2002).

The business case for privacy that we outlined in *The Privacy Payoff* focused, in essence, on gaining and keeping customer trust and loyalty, which, in turn, leads to repeat and higher-value business, and avoids "churn." Good privacy leads to solid ROI (return on investment). We also outlined how the privacy payoff could work in reverse: poor privacy practices could result in additional costs and foregone opportunities and revenues, along with a host of other negative consequences. These could include:

- harm to clients or customers whose personal data was used or disclosed inappropriately;
- costly damage to an organization's reputation and brand;
- financial losses associated with deterioration in the quality or integrity of personal data;
- financial losses due to a loss of business or delay in the implementation of a new product or service, due to privacy concerns;
- loss of market share or a drop in stock prices following negative publicity;
- violations of privacy laws and regulations;
- diminished confidence and trust in the industry.

The Privacy Payoff was followed by a joint publication between my office and Deloitte & Touche[16] that clarified the central issues and challenges for organizations, such as the critical distinctions and interplay between information security and privacy, and provided advice for developing strategies to enhance information security and privacy protections.

A year later, my office commissioned a study by the Ponemon Institute on corporate privacy practices.[17] The report compared what Canadian and U.S. companies were doing to achieve privacy programs and also looked at what companies were doing to move beyond simple compliance with regulations in order to build trusted relationships with stakeholders, increase revenue, and strengthen reputation and brand.

The study showed that leading companies were more likely to execute the following business practices as an integral part of their enterprise privacy program:

- Integrate information security and privacy into one virtual team
- Incorporate perspectives of legal, marketing, human resources and IT into privacy strategy

[16] Information and Privacy Commissioner/Ontario and Deloitte & Touche, The Security-Privacy Paradox: Issues, Misconceptions and Strategies. (2004), www.ipc.on.ca/images/Resources/sec-priv.pdf

[17] Information and Privacy Commissioner/Ontario and Ponemon Institute, Cross-National Study of Canadian and U.S. Corporate Privacy Practices. www.ipc.on.ca/images/Resources/cross.pdf

- Centralize privacy program responsibility under one senior executive sponsor
- Whenever feasible, consider using privacy enabling technologies,
- Empower local managers to get involved, especially in communications, training and outreach,
- Obtain real budget authority to implement enterprise programs,
- Build process standards that resemble six sigma or ISO programs,
- Establish upstream communication and fair redress,
- Conduct privacy impact assessments to objectively identify issues, problems and risks,
- Provide good reporting and disclosure tools to all stakeholders,
- Listen to customers about their privacy preferences, concerns and issues,
- Ensure both privacy goals and practical business objectives are met.

This practical understanding of what successful execution of privacy programs looked like from the inside would shape and focus my work over the next several years. As always, I seized opportunities to partner with thought leaders, captains of industry, privacy professionals, and government leaders. Through the 2000's, these opportunities were plentiful, and my office was busy!

We partnered, for example, with the Schulich School of Business at York University on a paper entitled *Privacy and Boards of Directors: What You Don't Know Can Hurt You*,[18] which argued that privacy protection starts at the top and must have a C-suite level presence to provide real and effective organizational accountability. The paper outlined specific steps businesses should take, including conducting a self-assessment, educating staff about privacy, appointing a Chief Privacy Officer, making privacy an integral part of performance evaluations and compensation packages, executing regular privacy audits, and asking senior management the right questions about privacy.

We also contributed, in 2005, to an international business research syndicate, led by Don Tapscott, which was investigating the changing shape of businesses and ways in which to achieve new competitive advantages by adopting strategic information technologies into and business practices. The resulting paper[19] outlined the five major privacy challenges facing organizations for the next generation and offered solutions based on our *Privacy by Design* approach.

In 2009, we partnered with leading US firms to describe and illustrate how *Privacy by Design* could be applied to enhance organizational accountability to, and

[18]Information and Privacy Commissioner/Ontario, Privacy and Boards of Directors: What You Don't Know Can Hurt You, http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=648

[19] Information and Privacy Commissioner/Ontario, Privacy and the Open-Networked Enterprise (2005), www.ipc.on.ca/images/Resources/priv-opennetw.pdf

compliance with, international privacy laws and other requirements.[20] This publication was one of a series of joint papers applying *Privacy by Design* principles to illustrative concrete case studies in diverse areas such as remote health care[21], biometric systems[22], and the emerging "smart grid."[23]

Throughout the mid to late 2000's, there were countless speaking engagements, publications, partnerships, think pieces, web resources, and working relationships being built. During this period, my focus remained the same: to lay the foundation for protecting privacy well into the future by encouraging, entreating, and enabling organizations to implement *Privacy by Design*.

2010: *Privacy by Design* Reaches a Tipping Point

By 2010, it was clear that the advocacy work of the past ten years was starting to pay off, as tremendous strides were made in evolving *PbD* from a conceptual framework into a practical one that was actually being applied by industry leaders. Organizations were no longer asking "why?" but "how?" The slide decks I had been using to present the business case for privacy went into retirement. They were replaced, instead, with slides about the growing momentum gathering behind *Privacy by Design*.

A high point for *PbD*, and for me personally, was the unanimous adoption of a landmark *Privacy by Design* resolution[24] by the full assembly of international Privacy Authorities and Regulators at the International Conference of Data Protection and Privacy Commissioners in Jerusalem.

---

[20] Ann Cavoukian, Ph.D., Marty Abrams, & Scott Taylor, Privacy by Design: Essential for Organizational Accountability and Strong Business Practices (2009), www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf

[21] Information and Privacy Commissioner/Ontario & HP Canada, RFID and Privacy: Guidance for Health-Care Providers (2008), http://www.ipc.on.ca/images/Resources/up-1rfid_HealthCare.pdf

[22] Ann Cavoukian, Ph.D., and Alex Stoianov, Ph.D., Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy (2007), http://www.ipc.on.ca/images/Resources/bio-encryp.pdf

[23] Information and Privacy Commissioner/Ontario and The Future of Privacy Forum, SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation, http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf; Information and Privacy Commissioner/Ontario, Hydro One, & Toronto Hydro, Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid, http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf; and Information and Privacy Commissioner/Ontario, Hydro One, GE, IBM & Telvent Operationalizing Privacy by Design: The Ontario Smart Grid Case Study, http://www.ipc.on.ca/images/Resources/pbd-ont-smartgrid-casestudy.pdf

[24] Information and Privacy Commissioner/Ontario, Landmark Resolution passed to preserve the Future of Privacy, http://www.ipc.on.ca/images/Resources/2010-10-29-Resolution-e_1.pdf

The resolution recognizes *Privacy by Design* as an "essential component of fundamental privacy protection." It also:

- Encourages the adoption of the principles of *Privacy by Design* as part of an organization's default mode of operation; and
- Invites Data Protection and Privacy Commissioners to promote *Privacy by Design*, foster the incorporation of its Foundational Principles in privacy policy and legislation in their respective jurisdictions, and encourage research into *Privacy by Design*.

To help support that work, I released a *Privacy by Design* Curriculum.[25] The Curriculum provides resources that enable virtually anyone to understand and *teach others* about *Privacy by Design* and how its principles may be applied in particular settings.

Furthering the work of implementation, I involved my office in several ground-breaking projects in this field. One of them, a joint paper[26] with the Ontario Lottery and Gaming Corporation (OLG), focused on a very novel application of *PbD* in the field of Biometric Encryption.

2010 also saw significant privacy gains through the application of *PbD* in other arenas. Near the end of 2009, for example, my office worked closely with Google to develop a tip sheet on encrypting Gmail messages. Through that process, Google decided, in early 2010, to set the default so that it automatically encrypted all email messages sent by users of its Gmail service – a significant advancement!

We also did some work on implementing *PbD* in the hot-button area of targeted advertising. This kind of advertising brings with it a host of privacy issues, from those directly connected with the practice (e.g. the tracking of online behaviour, the use of location data as reported by mobile devices, etc.) to broader, Internet-wide topics (e.g. IP addresses as personal information, etc.).

In October 2010, we issued a joint paper[27] on one facet of the rapidly-evolving field of targeted advertising: precise IP geolocation, and the potential role of ISPs in the ad serving model. Our paper described the innovative technology developed by a highly innovative company, Bering Media, Inc., which allows ISPs to partner with an

---

[25] All available at: www.privacybydesign.ca

[26] Information and Privacy Commissioner/Ontario, Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept, http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1000

[27] Information and Privacy Commissioner/Ontario, Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising, http://www.ipc.on.ca/images/Resources/pbd-ip-geo.pdf

ad server to provide IP geolocation services without *any* disclosure of personally identifiable information about subscribers. Using their privacy architecture, the ISP can partner with an ad server without the server reading or modifying any packets travelling through the ISP's network.

While these and other *PbD* projects spanned widely disparate fields, all of them demonstrated the extent to which *Privacy by Design* fosters innovation by challenging system designers and engineers to think creatively. These projects have confirmed what I have long held to be true: rejecting the widespread but misguided view that privacy and other objectives are necessarily in conflict, opens up a *world* of possibilities.

The Long Road Ahead: Launching a Decade of *Privacy by Design*

At the start of 2011, the Future of Privacy Forum, a Washington-based think tank that promotes responsible data privacy practices, posted its First Annual List of Privacy Ins and Outs. I was delighted (and gratified) to see *PbD* make the list of what's "in."

2010 was an excellent year for *Privacy by Design*. We had clearly reached a tipping point. But this is not the time to rest on our laurels. There is much to look forward to, and there is yet much work to be done. Indeed, I am predicting that this year will launch the decade of *Privacy by Design*, and put in place a solid foundation for assuring the future of privacy. Here are a few of the developments that I am hoping for and will be working towards in this decade:

1. PbD as a Fundmanetal Component of Privacy Frameworks

There is a growing momentum to enshrine the 7 Foundational Principles of *PbD* into privacy policies and regulatory frameworks. The U.S. Federal Trade Commission's noteworthy paper, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policy Makers*,[28] named *PbD* as one its three recommendations.

Similarly, the European Commission's (EC) recent consultation paper[29] proposed *PbD* as a way to enhance the responsibilities of organizations. Peter Hustinx, European Data Protection Supervisor, has said "Privacy by Design needs to be explicitly included as a general binding principle into the existing data protection legal framework. This would compel its implementation by data controllers and ICT

[28] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers, http://www.ftc.gov/opa/2010/12/privacyreport.shtm

[29] Consultation on the Commission's comprehensive approach on personal data protection in the European Union, http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm

designers and manufacturers while offering more legitimacy to enforcement authorities to require its effective application in practice...*Privacy by Design* should also be fully endorsed by the forthcoming European Digital Agenda and become a binding principle in future EU policies."[30]

In 2011, we are witnessing further movement toward embedding *PbD* into regulatory instruments, voluntary codes, and "best practices" all around the world. Among other things, this will significantly expand the understanding of how the principles of *PbD* may be interpreted in specific contexts, and applied to particular industries and technologies. And with the translation of the 7 Foundational Principles into 14 languages, *PbD* will truly become a global standard.[31]

2. PbD as a Fixture Within Public and Private Sector Ecosystems

The signs are already beginning to appear: market leaders are starting to embrace *Privacy by Design*, and are, in turn, reaping the benefits. Recently, thought leaders Don Tapscott and Anthony D. Williams, authors of *Macrowikinomics: Rebooting Business and the World*, joined the ranks of strong voices in support of *PbD*, in an article[32] urging companies to adopt its principles. "Cavoukian's Privacy by Design playbook explains how to build privacy protections into everyday business practices. Every business needs to design privacy principles and practices into their operations."

Organizations that act proactively stand to gain a sustainable competitive advantage from their early adoption of responsible information practices, and enjoy savings of time and resources by building privacy in from the outset, rather than trying to retrofit an ill-fitting solution, after the fact.

3. A Generation of "Privacy Heroes"

Over the past few years, my office's annual *PbD* Challenge[33], our Developers Challenge (co-sponsored with Microsoft) and the *PbD* Ambassador program have begun to stimulate and recognize emerging leadership in the area of *Privacy by Design*. Armed with forward vision, technical expertise and respect for consumers and citizens, a committed pool of individuals and organizations, who we call "privacy heroes" – including researchers, academics, engineers, regulators, captains of industry, and privacy advocates – are emerging as forerunners in the implemention of *Privacy by Design*.

---

[30] Privacy advisor calls for 'privacy by design' laws, http://www.out-law.com/page-10851

[31] The 7 Foundational Principles are being translated into a growing number of languages, including French, German, Italian, Spanish, Czech, Dutch, Estonian, Hebrew, Hindi, Chinese, Japanese, Arabic, Armenian, and Russian.

[32] Don Tapscott and Anthony D. Williams: Social media's unexpected threat, www.ctv.ca/generic/generated/static/business/article1854656.html

[33] Find information about the *PbD* Challenge at http://www.privacybydesign.ca/events/upcoming-events/

We look to these privacy heroes to expand the pool of *PbD* expertise, commitment, and innovation in 2011 and beyond, as the ranks of *PbD* supporters continue to swell.

4. Innovative Applications of PbD

2010 saw *PbD* grow from a conceptual framework to a practical methodology that organizations are increasingly implementing. Significant projects in the areas of Smart Grid[34] and Privacy-Protective Biometric Facial Recognition[35], and mobile applications[36] marked the beginning of true innovation in applying the principles of *Privacy by Design*.

With market leaders like GE, HP, IBM, Microsoft, Oracle, Intel, Hydro One, the Ontario Lottery and Gaming Corporation, and new talent like Bering Media paving the way, 2011 promises to be a banner year for new and innovative applications of *PbD*.

5. Consistent Alignment between Business Practices and Consumer Expectations

Many organizations have lengthy, "legalistic" privacy policies that are difficult for consumers to read, let alone understand. Nonetheless, many consumers assume – incorrectly – the fact that a site posts a policy means that it will not share their personal information with unauthorized third parties. These expectations are certainly not well-founded, nor are they always consistent with current business practices.

Embedding privacy proactively will bring business practices into much better alignment with consumer expectations. While this process may take some time, I think we can look forward to seeing many positive steps in the coming year. And that will be good for everyone – consumers **and** businesses – because when consumers trust that their personal information is being protected, they will continue to support the growth of new forms of web-based commerce, without fearing for their

---

[34] Information and Privacy Commissioner/Ontario, Hydro One, & Toronto Hydro, Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid, http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf and Information and Privacy Commissioner/Ontario, Hydro One, GE, IBM & Telvent Operationalizing Privacy by Design: The Ontario Smart Grid Case Study, http://www.ipc.on.ca/images/Resources/pbd-ont-smartgrid-casestudy.pdf

[35] Information and Privacy Commissioner/Ontario and Ontario Lottery and Gaming Corporation, Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept, http://www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf

[36] Information and Privacy Commissioner/Ontario & Arizona State University's Privacy by Design Research Lab, The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users. (2010), http://www.ipc.on.ca/images/Resources/pbd-asu-mobile.pdf

information. Consumer confidence and business development – positive sum, win/win!

The road behind me may feel like a long one, but it has only just begun. Along the way, the cause of *Privacy by Design* has been greatly helped by our allies, partners, collaborators, and colleagues. Together we have fought to retain the ability to continue to enjoy privacy while enjoying the benefits of the modern age, win/win, not zero-sum.

The road ahead promises to be just as long. I invite all of you to join me in realizing the vision of a future world where privacy lives on by striving to implement innovative *Privacy by Design* solutions in your own organizations and lives. Our freedom and privacy may be at stake – what could be more important?