Privacy by Design in Law, Policy and Practice

A White Paper for Regulators, Decision-makers and Policy-makers

Foreword by:
Pamela Jones Harbour,
Former Federal Trade Commissioner

August 2011

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner,
Ontario, Canada

Acknowledgements

I am deeply indebted to Pamela Jones Harbour, who was instrumental in developing some of the key ideas that shaped this paper, and in crafting an earlier version of it. Her depth of experience, her thoughtfulness, and the wisdom she brings as a former Federal Trade Commissioner were invaluable. I greatly appreciate Pam's support, and applaud her leadership!

Many thanks also to Ken Anderson, Sandra Kahale, and Stephen McCammon of my office, for their work on this paper.

Information and Privacy Commissioner, Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Privacy by Design in Law, Policy and Practice

A White Paper for Regulators, Decision-makers and Policy-makers

"*Privacy by Design* is an excellent idea. Designing administrative means to protect personal privacy before it is breached is a welcome addition to the tools for protecting this vitally important human value."

The Honourable Justice Gérard Vincent La Forest, QC
Justice of the Supreme Court of Canada, 1985-1997

Table of Contents

Foreword
Pamela Jones Harbour

New technology can create unique challenges for individual privacy rights and provide novel complications for regulators looking to preserve both privacy rights and technological innovation. Society has long puzzled over how best to design regulatory frameworks that balance privacy rights and emerging technologies. Indeed, as early as 1890, when newspaper and photograph technologies were beginning to ascend, legal scholars called for added privacy protections, including enshrining those rights in the criminal law. Protecting privacy, a "right most valued by civilized men," while still promoting innovation, has never been more challenging than it is in an increasingly online and technology focused world. Now, more than ever, information can cross many nations' borders in a mere instant, and consumers' movements and activities can be tracked through their computers and mobile phones. At the same time, technological innovations can improve lives, increase public safety, build wealth, and promote efficiencies in how we use scarce resources. Just as there is value in information to researchers, marketers, corporations, and governments, there is an equally important value in privacy to the individual. Consequently, managing privacy and technological innovation is important to the global economy and is best addressed by a comprehensive and flexible approach.

Governmental privacy protections alone, such as enhanced criminal laws and administrative policies, can overly restrict innovation and under protect individual privacy rights. In fact, such governmental protections can become ceilings for both individual privacy protections and innovation – in part because they are reactive in nature and often slow to change. At the same time, without some guiding standards, it is difficult for technological innovators to define the competitive field of play and balance the risks and rewards. Accordingly, there must be some balance between regulation and innovation. One way to achieve that harmony is to embed privacy features from the beginning, starting with the design specifications of new technologies, i.e., *Privacy by Design* (*PbD*).

PbD has permeated the privacy arena in many respects. In the United States, for example, the Federal Trade Commission ("FTC") has recommended this approach to protecting privacy. The FTC has emphasized that "companies should adopt a 'privacy by design' approach by building privacy protections into their everyday business practices." To that end, the FTC has stressed the need for fully integrated privacy measures that carry through the entire data lifecycle, employee training and oversight on privacy issues, and customized privacy practices scaled to the sensitivity of the data at issue. Such concepts are not new, but the time has come for industries to implement them systematically.

Undoubtedly, there is a wide array of reasons for the FTC to make these recommendations. In my view, the most compelling reason for incorporating *PbD* in an organizational framework is its proactive approach to privacy. Traditionally, privacy regulation has been largely reactive, that is, it was only triggered once a privacy breach occurred. Conversely, by implementing a proactive, self-policing approach to privacy, an organization should be able to avoid many privacy issues and have in place tools to remedy potential breaches of privacy.

An organization that has failed to prevent a privacy issue, however, can still incorporate *PbD* principles in its remediation efforts. For example, in March 2010, Google agreed to a proposed consent decree to settle the FTC's investigation into alleged privacy lapses in Google's new social networking service, called Buzz. The allegations included failure to fully disclose the social network's default privacy settings to new users, and that its opt-out feature failed to fully remove the user from the Buzz network. As part of the proposed consent decree, Google agreed to implement a comprehensive privacy program that includes the designation of Google employees responsible for the company's implementation and compliance with acceptable privacy practices. Google is also required to consider privacy compliance in its selection and retention of service providers. Furthermore, for the next twenty years, a third party auditor, selected by Google but approved by the FTC, will conduct biennial audits of Google's privacy compliance and report the results of its investigation to the FTC.

There is growing momentum to embody *PbD* and its seven foundational principles in privacy policies and regulatory frameworks. But incorporation of *PbD* in a country's legislative body is not without its challenges. Not only must a country explore what kinds of instruments are appropriate but also how to interpret *PbD*. In the process, nations must always consider that *PbD* provides a baseline for embedding privacy considerations into legislation, and that *PbD's* presence throughout the business world is becoming more and more the norm.

Pamela Jones Harbour was a U.S. Federal Trade Commissioner from 2003 until 2010. Ms. Harbour is now a partner at the international law firm of Fulbright & Jaworski L.L.P., where she heads the firm's Privacy, Competition and Data Protection practice group. Ms. Harbour is well recognized for her knowledge of evolving areas of competition and consumer protection law, including privacy and data security issues. Ms. Harbour's offices are located in Washington, D.C. and New York.

Introduction:
The Growing Momentum behind *Privacy by Design*

Privacy by Design (*PbD*) is an approach to protecting privacy by embedding it into the design specifications of information technologies, accountable business practices, and networked infrastructures, right from the outset. It was developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, in the 1990s, as a response to the growing threats to online privacy that were beginning to emerge at that time.

PbD represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches, after-the-fact. Alexander Dix, Berlin Commissioner for Data Protection and Freedom of Information, has described these traditional approaches as "locking the stable door after the horse has bolted."[1]

By contrast, *PbD* requires an evolution in the way that organizations think about privacy – moving from a reactive mode to a proactive one. Similarly, enshrining *PbD* in regulatory instruments, voluntary codes, and best practices requires an evolution in how policy and law makers approach privacy rule-making.

The rapid pace of technological change is making traditional approaches to privacy regulation increasingly untenable. The emergence of *PbD* as the new generation of privacy protection invites the development of innovative approaches to promoting and enshrining it in instruments of various kinds, including regulatory ones.

The time is ripe for this kind of innovation. Over the past several years, momentum behind *Privacy by Design* (*PbD*) has been steadily growing. It is increasingly becoming a "basic principle" of data protection.[2] Global and local businesses alike are starting to implement the 7 Foundational Principles of *PbD*,[3] with mounting interest among regulators and policy-makers in enshrining these principles in privacy policies and frameworks, around the world.

Significant developments in this area include the unanimous adoption, in 2010, of a landmark *Privacy by Design* resolution by international Privacy Authorities and Regulators at the International Conference of Data Protection and Privacy Commissioners in Jerusalem.[4] The resolution recognizes *Privacy by Design* as an "essential component of fundamental privacy protection" – an International Standard, and urges its adoption in regulations and legislation around the world.

1 Alexander Dix, Built-in Privacy – no panacea but a necessary condition for effective privacy protection. Privacy by Design Issue of Identity in the Information Society Volume 3, Number 2, (August 2010). p 257.

2 Peter Hustinx, Privacy by design: delivering the promises. Privacy by Design Issue of Identity in the Information Society Volume 3, Number 2, (August 2010). p 254.

3 Market leaders like Hydro One, Toronto Hydro, GE, IBM, Intel, the Ontario Lottery and Gaming Corporation, and Bering Media have been leading the way. For more information about their activities, see www.ipc.on.ca.

4 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

A year earlier, the EU Article 29 Data Protection Working Party and the Working Party on Police and Justice issued a joint Opinion, advocating for incorporating the principles of *PbD* into a new EU privacy framework.[5] In November 2010, an EC consultation paper followed on this work and called for the promotion of possibilities for the "concrete implementation of the concept of '*Privacy by Design*.'"[6] This was echoed in March 2010, with the European Data Protection Supervisor recommending to "include unequivocally and explicitly the principle of *Privacy by Design* into the existing data protection regulatory framework."[7]

Momentum has been similarly gathering in the United States. Through 2009 and 2010, the U.S. Federal Trade Commission (FTC) hosted a series of public roundtable discussions on privacy issues in the digital age.[8] In its submission, the Center for Democracy and Technology recommended that the FTC foster the adoption of business practices consistent with *PbD* principles.[9] The subsequent FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, proposed a framework for business and policymakers that features *PbD* principles as core values, and highlighted *PbD* as one of its three key recommendations.[10]

PbD also appeared, for the first time, in federal privacy legislation proposed by Senators John Kerry (D-MA) and John McCain (R-AZ) in 2011. If passed, their *Commercial Privacy Bill of Rights*[11] would require businesses that collect, use, store or transfer consumer information to implement a version of *Privacy by Design* when developing products, and provide consumers with real choices about how data are used, collected and shared.[12]

The *Commercial Privacy Bill of Rights* was only one of many recent legislative initiatives in the U.S., which included, for example:

- *BEST PRACTICES Act*, H.R. 611 (Rep. Rush): introduced Feb. 10, 2011. Referred to the House Subcommittee on Commerce, Manufacturing, and Trade.
- *Consumer Privacy Protection Act of 2011*, H.R. 1528 (Reps. Stearns, Matheson, Bilbray, and Manzullo): introduced Apr. 13, 2011. Referred to the House Subcommittee on Commerce, Manufacturing, and Trade.
- *Do Not Track Me Online Act*, H.R. 654 (Rep. Speier): introduced Feb. 11, 2011. Referred to the House Subcommittee on Commerce, Manufacturing, and Trade.

---

5 Article 29 Data Protection Working Party and Working Party on Police and Justice, The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data. 02356/09/EN, WP 168 (Dec. 1, 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf. p. 2-3, 6, 8, 12-15, 27

6 European Commission, *Ibid* note 3, at 12.

7 European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy. (Mar. 18, 2010), http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf at p. 8. See generally *supra* at p. 2, 4-11, 18-19, 21.

8 FTC Roundtable Series, *Exploring Privacy*, (Mar. 2010), http://www.ftc.gov/bcp/workshops/privacyroundtables

9 Center for Democracy and Technology, Comment, *The Role of Privacy by Design in Protecting Consumer Privacy*, (Dec. 21, 2009), http://www.ftc.gov/os/comments/privacyroundtable/544506-00067.pdf

10 Federal Trade Commission (Bureau of Consumer Protection), Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policy Makers*, at v, 41 (Dec. 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

11 John Kerry, US Senator for Massachusetts, Commercial Privacy Bill of Rights. http://kerry.senate.gov/work/issues/issue/?id=74638d00-002c-4f5e-9709-1cb51c6759e6&CFID=90056053&CFTOKEN=63781113

12 Cynthia Larose, Kerry and McCain Introduce Commercial Privacy Bill of Rights. Privacy and Security Matters (April 13, 2011) http://www.privacyandsecuritymatters.com/2011/04/post/

- *Do-Not-Track Online Act of 2011*, S. 913 (Sen. Rockefeller): introduced May 9, 2011. Referred to the Senate Committee on Commerce, Science, and Transportation.
- *Do Not Track Kids Act of 2011*, H. R. 1895 (Reps. Markey and Barton): introduced May 13, 2011. Referred to the House Committee on Energy and Commerce.
- *Geolocation Privacy and Surveillance Act*, H.R. 2168 (Reps. Chaffetz and Goodlatte): introduced June 14, 2011. Referred to the House Committee on the Judiciary and the House Committee on Intelligence (Permanent Select).
- *Geolocation Privacy and Surveillance Act*, S. 1212 (Sen. Wyden): introduced June 15, 2011. Referred to the Senate Committee on the Judiciary.
- *Location Privacy Protection Act of 2011*, S. 1223 (Sens. Franken and Blumenthal): introduced June 16, 2011. Referred to the Senate Committee on the Judiciary.
- *Electronic Communications Privacy Act Amendments Act of 2011*, S. 1011 (Sen. Leahy): introduced May 17, 2011. Referred to the Senate Committee on the Judiciary.
- *Financial Information Privacy Act of 2011*, H.R. 653 (Reps. Speier, Hastings, and Filner): introduced Feb. 11, 2011. Referred to the House Subcommittee on Financial Institutions and Consumer Credit.

There has also been a great deal of activity in the related area of breach notification. Breach notification legislation has been enacted in 46 U.S. States. Ontario's *Personal Health Information Protection Act* also includes mandatory breach notification provisions. And the EU is considering rules to govern the behaviour of companies when breaches occur. These types of provisions are important in ensuring transparency and alerting individuals to the possible risks flowing from their personal information being compromised. They are, however, essentially reactive in nature.

Organizations that are subject to breach notification laws should be especially motivated to adopt a proactive *Privacy by Design* approach, which will help them to avoid data breaches in the first place, and thereby minimize their obligations under breach notification legislation. By addressing privacy at the outset, these organizations can minimize the need to address it reactively, at which time they risk damage to their reputations, as well as their bottom lines. By addressing privacy at the outset, organizations can minimize the need to address problems reactively, when they risk damage to their reputations, as well as their bottom lines.

Given the mounting momentum behind *PbD*, and the growing interest in incorporating its principles into policy, practice, and regulation, there is an emerging appetite among policy-makers, regulators, and decision-makers for resources that support these objectives. This white paper is intended to serve as just such a resource, supporting key players in identifying the range of instruments that *PbD*, which is flexible, proactive, and technology-neutral, may be usefully incorporated into, and developing an understanding of how best to reflect *PbD*'s underlying philosophy in these instruments.

Context: Privacy in Modern Times

The Meaning of Privacy

In 1890, future U.S. Supreme Court Justices Samuel Warren and Louis Brandeis, described privacy as the "the right to be let alone."[13] They identified it as the right that enables individuals to have personal autonomy, freedom of association, moments of reserve, solitude, intimacy, and independence.

Almost 100 years later, as the computer era was dawning, a new subset of privacy – "informational privacy," was articulated and defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[14] As a concept, it is predicated on "the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain ... as he sees fit."[15]

We consider privacy to revolve around control – personal control over the collection, use, and disclosure of one's personally identifiable info, similar to the German concept of "informational self-determination," which was first used in the context of a German constitutional ruling relating to personal information collected during the 1983 census.

As the underpinning of many of the rights and freedoms we hold dear, privacy has long been – and still remains – a vital component of free and democratic societies. It is "[g]rounded in man's physical and moral autonomy" and "essential for the well-being of the individual."[16]

Our increasingly technologically-driven world, however, puts tremendous pressure on privacy. As early as 1890, when newspaper and photography technologies were in their infancy, legal scholars were decrying their impacts, and calling for new legal protections for privacy.[17] Today, what has fundamentally changed is that practical obscurity – the basis for privacy norms throughout much of history – is fast disappearing. The functional impediments to surveillance that once protected our privacy, by default – such as data processing and storage costs, and the difficulty of linking files from multiple databases – are becoming increasingly irrelevant. At the same time, oceans of personal information are being created. Meaningful informational self-determination is becoming increasingly difficult to achieve.

And yet our need for privacy, the reflection and solitude it allows us to enjoy, as well as the opportunity it allows for the protected practice of political rights to speech, dissent, and association, is as relevant now as it has ever been. Indeed, it is perhaps *more* relevant, and increasingly necessary, now that our lives are so networked, interconnected and, indeed, "plugged in."

13 Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*. Harvard Law Review 4, 193-220 (1890)
14 Alan Westin, Privacy and Freedom. Atheneum, New York. (1967).
15 *R. v. Tessling*, [2004] S.C.J. No. 63 at para. 23, quoting the Report of a Task Force established jointly by Department of Communications/Department of Justice, Privacy and Computers (1972), at p. 13
16 R. v. Dyment, [1988] 2 S.C.R. 417, at p. 427
17 Ibid. "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"

How can we sustain and support the myriad benefits of technological innovation, such as access to extraordinary new services, conveniences, and efficiencies, while at the same time preserving the privacy that is so essential to our freedom and autonomy? Read on.

Evolution in the Meaning and Expectation of Privacy

20 years ago, it was popular to think of privacy as simply a personal good (not also a societal one), and so a matter of *individual responsibility*. If you valued your privacy, the onus was on you to take steps to protect it. But changes in information technologies and their uses over the past few decades have made it increasingly difficult for individuals to exert meaningful control over their personal information.

Historically, at about the time when information technologies began to take off, a number of other factors combined to put pressure on organizations to provide better privacy assurances.[18] Growing interest in electronic commerce, for example, shone a new spotlight on privacy. It became clear that 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.

By the early '90s, there was considerable public discussion about the merits of good privacy practices, some of which flowed from the anticipated coming into force of the European Data Protection Directive.[19] 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.

As momentum gathered around these issues through the early 90s and into the 2000s, many jurisdictions passed privacy laws or started promoting privacy practices based on the recognition that individuals had an interest in the processing of their personal data. These laws and practices were founded on Fair Information Practices (FIPs) – universal privacy principles for handling personal data.

First fully codified by the OECD in 1980,[20] there are many articulations of Fair Information Practices, including the EU Directive on Data Protection, The Canadian Standards Association's Privacy Code, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, the U.S. Safe Harbor Principles, and the Global Privacy Standard.[21] 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

18 Ann Cavoukian and Don Tapscott, Who Knows: Safeguarding your Privacy in a Networked World. Random House, Toronto (1995), describes these pressures in detail.

19 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)

20 An earlier, partial set of Fair Information Practices were drafted by an advisory committee of the Department of Health, Education, and Welfare (HEW) in 1973. See Cavoukian and Tapscott, p. 37.

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

other than those for which it was collected, except with the consent of the individual or as authorized by law;

- **User Participation and Transparency** – individuals should be empowered to play a participatory role in the lifecycle of their own personal data and should be made aware of the practices associated with its use and disclosure; and
- **Strong security** – the confidentiality, integrity and availability of personal data should be safeguarded, as appropriate to the sensitivity of the information.

Fair Information Practices have been essential in providing a starting point for responsible data management practices. But many organizations have described them as regulatory burdens, and approach compliance with them as necessarily stifling innovation and impairing a free competitive marketplace. Viewed from such a zero-sum perspective, where the task is seen as a "balancing" act of competing business and privacy requirements, either privacy or functionality loses out.

However, the zero-sum/balancing perspective that such organizations operate under is sadly misguided. As Julian Sanchez argues in a 2011 blog posting, balance metaphors ultimately lock both sides into unwinnable arguments about the relative merits of "competing" values. They 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.[22] This certainly need not be the case, and approaching the issue from this angle tends to prevent one from engaging creatively in achieving substantial success for *both privacy* **and** innovation.[23]

Moreover, the balancing perspective has stimulated an overemphasis on notice and consent as the primary vehicle for addressing issues related to the management of personal information, diluting the true privacy potential of FIPs. As the U.S. Department of Commerce notes, "Under the current notice-and choice model, consumers' privacy rights depend on their ability to understand and act on each individual company's privacy policy. These documents "are generally written in legalese that is unintelligible to the average consumer." As a result of the number and complexity of such notices, this situation is "typically overwhelming to the average consumer." The result… is a lack of transparency into actual privacy practices and a diminished ability of consumers to make informed choices."[24]

Increasingly, organizations that have anchored their privacy program in legalistic interpretations of FIPs, focusing on consumer consent as the foundation of their approach, are finding themselves at odds with consumer *expectations* about how personal information is to be handled. These organizations have approached privacy as a compliance issue. But, in fact, privacy is becoming a business issue, and its protection is becoming an important aspect of an organization's ability to inspire and maintain consumer confidence, trust, and loyalty.

---

22 Julian Sanchez, www.juliansanchez.com (blog posting February 4, 2011), 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.

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

24 Department of Commerce (Internet Policy Task Force), Green Paper: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework. (Dec. 2010), p 31-32. http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf

This emerging reality is apparent in a forthcoming paper by Kenneth A. Bamberger and Deirdre K. Mulligan, which presents findings from the first study of corporate privacy management in 15 years, involving qualitative interviews with leading Chief Privacy Officers.[25] The authors note that "between 1995 and 2010, corporate privacy management in the United States has undergone a profound transformation."[26] Thousands of companies have created Chief Privacy Officer (CPO) positions, and these CPOs report a profound shift in the definition of privacy and its treatment over that period. "Privacy, in respondents' language, has evolved over the last several years to be defined in large part by respect for what consumers expect regarding the treatment of their personal sphere."[27]

Their findings suggest that, in the corporate context, the meaning of true privacy increasingly depends on "the beliefs and assumptions of consumers as to the appropriate treatment of individual information and personal identity – expectations that evolve constantly and change by context. The success of privacy protection, then, [must] be measured not by the vindication of notice and consent rights, but in the actual prevention of substantive harms, such as preventing data breaches, or treating information in a way that protects the "trust" of those whose information is at stake."[28] Enter *Privacy by Design*, who's raison d'etre is to prevent the harm from arising.

No less critically, industry leaders are beginning to realize that effective privacy programs are an essential component of creating and sustaining trusting, long-term relationships with existing customers, while forming the basis for attracting opportunity in the form of new ones. This realization is fostering a perspective on privacy that is expansively consumer-driven, rather than narrowly legalistic.

At the same time, industry is being confronted with mounting evidence that privacy breaches can have profound and long-term negative consequences, including financial ones, not only for individuals but also for organizations.[29] Forward-thinking organizations are thus becoming highly motivated to take privacy seriously as part of their risk management activities. In this environment, adherence to FIPs is a necessary, but not sufficient, condition. As one Chief Privacy Officer has said, "The end objective in my mind is always what's the right thing to do to maintain the company's trusted relationship with our employees, with our clients, with any constituency in society that has a relationship to us."[30]

25 Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Books and on the Ground – Draft. http://ssrn.com/abstract=1568385. To be published in Stanford Law Review, vol. 63 (2011).
26 Bamberger & Mulligan, p. 105.
27 *Ibid*, p. 105.
28 *Ibid*, p. 105-6.
29 There are countless examples of this. See, for example, Sara Schmidt, 'BreachFest' may sound funny, but expert says digital security has been a concern for years. Postmedia News. (June 6, 2011) www.canada.com. Sony experienced several breaches in 2011; costs related to those breaches are estimated at $173 million (U.S.) -- an 18% reduction out of their bottom line. Michael Lewis, Honda hacked as Sony reels. Toronto Star. (May 27, 2011).
30 *Ibid*, p. 125.

Privacy by Design: The Next Generation of Privacy Protection

As our technological reality evolves, with our experience and expectations of privacy evolving alongside it, the strategies that we pursue in order to secure the privacy that is so fundamental to our freedom and autonomy must also evolve.

FIPs continue to provide an important anchor, but we must go further to achieve the meaningful privacy objectives that underlie them. Just as FIPs evolved to protect against the early impacts of the growth of information technologies 30 years ago, new privacy protections, perhaps articulated in new ways, are now needed to respond to today's emerging reality.

The current challenges to privacy are driven by the synergy between the fundamentally positive forces of innovation, competition, and the worldwide adoption of new information technologies. The solution, therefore, must be woven or baked in to these synergetic forces. Privacy must become the default mode of design and operation.

This is precisely the aim of *Privacy by Design* (*PbD*) – the philosophy and methodology of embedding privacy into the design specifications of information technologies, business practices, and networked infrastructures as a core functionality. *Privacy by Design* means building in privacy right up front, directly into the design specifications and architecture of new systems and processes.

Privacy by Design is based on 7 Foundational Principles (see Appendix A). While these principles grow out of FIPs, they go much farther, emphasizing respect for user privacy and the need to embed privacy as the default while preserving a commitment to full functionality in a win-win, positive-sum approach. As such, it encourages a focus not on mere technical compliance, but rather on approaching privacy holistically, as a design feature of an entire organization's activities and processes. Indeed, in the words of Peter Schaar, German Data Protection Commissioner, "*PbD* should not be limited to developing clever technical solutions and incorporating them into systems. It is equally important to examine very early in the planning process whether and how to limit the amount of personal data to the absolute minimum necessary. The tendency to reproduce increasingly complicated bureaucratic systems in information technology can be seen in other IT processes and can lead to major problems for data protection. This risk exists even when great efforts are made to ensure data protection [security] and prevent data misuse."[31]

PbD embeds respect for privacy deeply and meaningfully across the organization, supporting achievement of a much higher privacy standard than implementation of FIPs has generally provided to date.

This aligns *PbD* with the reality that the demands of the marketplace are transforming consumer privacy from a policy or compliance issue into a business issue. Getting privacy right is becoming increasingly critical to achieving success in the new economy. In this environment, *PbD* offers a principled, flexible, and technology-neutral vehicle for engaging with privacy issues, and for resolving them in ways that support multiple outcomes in a positive-sum, win-win scenario.

31 Peter Schaar, Privacy by Design. Privacy by Design Issue of Identity in the Information Society Volume 3, Number 2, (August 2010). p 273.

This approach is a significant break from traditional ones, which have tended to posit privacy as either an impediment to business development and innovation or, at best, an afterthought. Instead, *PbD* invites organizations to weave privacy creatively into business practices, technologies, and networked infrastructures, in such a way that it becomes part of how the organization operates.

In support of this ambitious agenda, *PbD* is necessarily flexible. There is no single way to rollout *Privacy by Design*. Rather than being prescriptive about outcomes, it encourages organizations to adopt a principled approach to decision-making, and to overall process and system design. Thus the process and outcome may be different in each organization that undertakes to implement it. Context is key – it matters enormously. The common thread, however, is that the outcome will be win-win – i.e. respectful of consumer privacy while achieving full functionality.

This recognizes and supports – in a way that FIPs alone do not seem to have been able to – the organization's own interest in leveraging privacy as an opportunity, rather than submitting to it as a burden. Approached from the perspective of an opportunity to innovate, privacy programs can have myriad benefits, including:

- Improved customer confidence, trust, and loyalty;
- Efficiencies and risk reduction flowing from handling only the personal information that is necessary to the business process;
- Competitive advantage in the marketplace;
- Cost savings as a result of building privacy in up front rather than having to bolt it on, after the fact;[32] and
- Significant reduction of exposure to liability associated with privacy breaches.

This is true regardless of whether the organization is operating in a regulated or unregulated environment with respect to privacy, or whether the applicable regulatory framework includes specifically. No matter what the requirements, *PbD* will help organizations to meet and exceed them by fostering responsible privacy practices throughout the organization, at every level.

A Positive Approach to Privacy: Implications for Regulators and Policy-makers

As a framework for effective privacy protection, *PbD*'s focus goes beyond strict technical compliance, encouraging organizations instead to use *PbD* to both drive and demonstrate their commitment to privacy. In much the same way that car manufacturers are beginning to seize upon emission standards as an opportunity to do more to position themselves as supporting a green future, organizations that handle personal information can leverage *PbD* to spur value-added innovation in the privacy arena.

As outlined above, rather than focusing solely on outcomes, *PbD* is also concerned with processes. For regulators and policy-makers, *PbD* invites a shift in how the privacy issue is approached. As Lawrence Lessig has said, "It may well be difficult for the government to regulate behavior directly,

32 Doug Westlund, CEO of N-Dimension Solutions, has said that "... building privacy and security functions into a Smart Grid system after it has been built costs 3 to 5 times as much."

given the architecture of the Internet as it is. But that doesn't mean it is difficult for the government to regulate the architecture of the Internet as it is."[33]

Incorporating *PbD* in policy, law, and practice translates into taking an approach to privacy that is both broader, and yet more flexible than traditional ones. It means requiring that privacy be woven into business processes in much the same way that other core societal values such as fairness, transparency, and proportionality, are. It means getting at privacy at a much deeper level – at the actual level of code, default settings, and operating systems – than ever before.

In the words of Professor Lessig:

> "For citizens of cyberspace, . . . code . . . is becoming a crucial focus of political contest. Who shall write that software that increasingly structures our daily lives? As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed. They are the ones who set its nature. Their decisions, now made in the interstices of how the Net is coded, define what the Net is."[34]

Approaching privacy from the level of code is a significant shift from traditional ways of thinking about data protection. So just as *PbD* represents a shift in the way that organizations must think about privacy – moving from a reactive model to a proactive one – enshrining *PbD* into regulatory instruments, voluntary codes, and best practices, requires a shift in how law and policy makers approach rule-making in this area. *PbD* represents the new generation of privacy protection – it invites the development of innovative approaches to promoting and enshrining privacy in various instruments.

In the next section, we take these themes further and examine specific approaches to incorporating *Privacy by Design* into policy, practice, and regulation.

33 Lawrence Lessig, Code 2.0. http://codev2.cc/download+remix/Lessig-Codev2.pdf p. 61
34 Ibid, p. 79.

Approaches to Incorporating *Privacy by Design*

With momentum growing behind enshrining the 7 Foundational Principles of *PbD* in privacy policies and frameworks around the world, the time is ripe for regulators, policy-makers, and industry leaders to open a dialogue about the range of instruments that *PbD* lends itself to, and how *PbD* may be incorporated, in ways that preserve its flexible, positive-sum characteristics.

Instructions embedded into software and hardware make cyberspace what it is – they are its architecture.[35] *PbD* offers a framework for influencing, shaping, and regulating this architecture in ways that recognize multiple legitimate functionalities, including privacy among them.

As Lawrence Lessig argues, multiple constraints can impact how something is regulated, including the law, social norms, the market, and architecture.[36] All of these are relevant, and operate in inter-related ways, in the context of privacy. For our purposes here, however, the focus is on law, and how law can be applied to influence architecture.

Initial considerations for decision-makers may be location and scope. Where and how should *PbD* be incorporated? Should it be implemented on a sector-by-sector basis or more broadly, throughout the business-consumer information ecosystem? Should it, for example, be a legislated requirement, a safe habor-type opportunity, or an instrument that individual organizations within the business community may choose to adopt?

Each approach will produce a different outcome. Adoption of *PbD* by individual organizations, for example, is useful in building business and competitive advantages for that organization. It may not, however, be sufficient for creating widespread consumer confidence in an industry or in a business, generally.

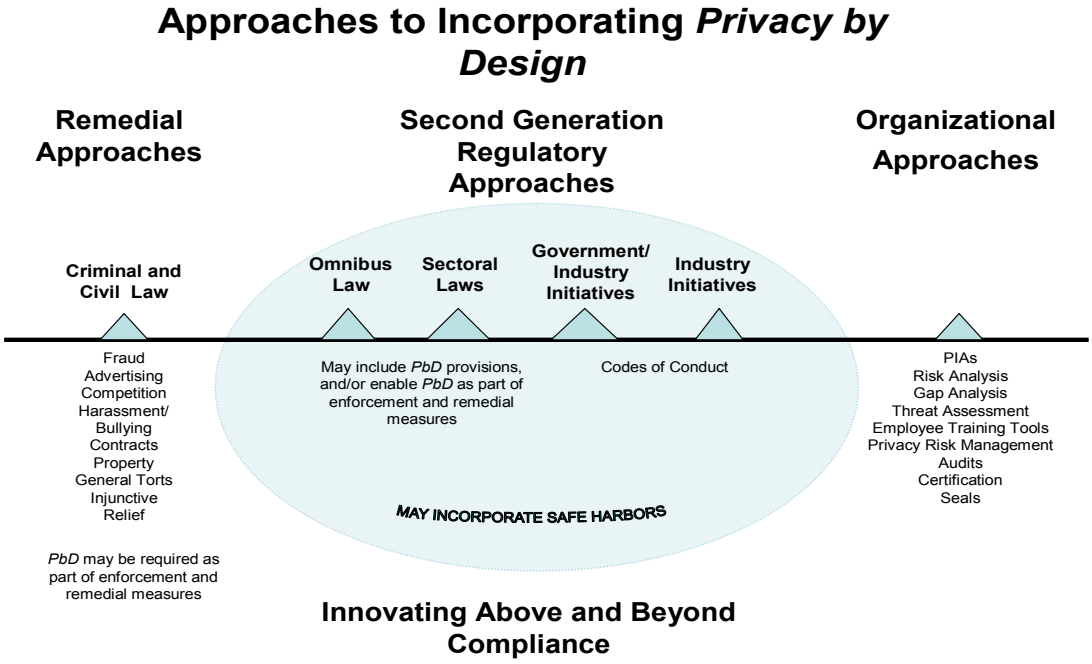
Sector-specific approaches, by contrast, can to help create trust and confidence in a particular industry, and shape the future direction of development in a way that aligns with consumer values around privacy. When *PbD* is applied across the whole business-consumer information ecosystem, it can create the foundation for widespread consumer confidence and trust, and spur innovation across all sectors of the economy. In addition, applying it remedially, for example through enforcement orders, may also be appropriate in certain circumstances.

Regulators and policy-makers must have a clear sense of their objectives in promoting *Privacy by Design* when considering the wide range of regulatory-related tools available, and the ways in which these tools can be usefully combined. Knowing that there are a range of soft and hard law techniques available, decision-makers can develop and apply governance models to "exploit market, corporate, and advocacy capacity to develop collective understanding of risk, and solutions to [present] and future privacy problems."[37]

The chart below summarizes a particular way of looking at the range of available instruments for encouraging the operationalization of the 7 Foundational Principles of *Privacy by Design*.

35 Lessig, p 121. Lessig provides many examples of how law can change the regulation of architecture, including the impact of the *American with Disabilities Act*, and car safety standards. See Chapter 7.
36 Ibid, p 123.
37 Bamberger, p 168.

These instruments and approaches are not mutually exclusive. They may – and sometimes must – be used in combination. But we consider them separately below in order to tease out the important differences between them.



Organizational Approaches to *PbD*

Adoption of *PbD* by an individual organization is very useful in building business and competitive advantages for that organization. It can also form an important part of an organization's privacy program in regulated or self-regulated environments.

Optimally, *PbD* should not be implemented on a piecemeal, project-by-project basis, but rather, across the entire organization. In practice, of course, privacy innovation may initially occur on a project basis, driven from the bottom up. The danger of such an approach in the long term, however, is that while a specific process or project may be privacy-protective, the entire organization may not be, which leads to spotty and, ultimately, unsatisfactory implementation of privacy, from a consumer perspective.

Project-by-project implementation of *PbD* should not, therefore, be considered other than as an interim step in the full rollout of *PbD*. In a full rollout, *PbD* should be applied across the board to IT systems, accountable business practices, physical design and networked infrastructure, touching every aspect of an organization.

Experience suggests that the successful implementation of *PbD* requires executive-level commitment to fostering the growth of a *Culture of Privacy*, which then enables sustained collective action by providing people with a similarity of approach, outlook and priorities. This leads privacy to be woven into the fabric of day-to-day operations of the organization, at all levels. Further, executives have an essential role to play in interpreting and implementing *Privacy by Design*'s flexible principles, in

ways that resonate with the organization's management structures and processes, as well as their understanding of customer and stakeholder expectations of privacy within their own particular industry. Using *PbD* as a framework, the organization can think critically about how to develop doubly-enabling, win-win solutions that are applicable and appropriate given the size and nature of the organization, the personal information it manages, and the range of risks, opportunities, and solutions available.

In applying *PbD* at the organizational level, organizations may choose to leverage any number of tools, including Privacy Impact Assessments (PIAs), risk management processes, and external validation programs involving privacy audits, seals and/or certifications.

Privacy Impact Assessments (PIAs)

A PIA is one of many tools used to help organizations ensure that the choices made in the design of a system or process meet the privacy needs of that system, typically by way of a directed set of questions, based on privacy requirements.[38] It can be an excellent entry point for applying the principles of *Privacy by Design*.

In some circumstances, a PIA may be conducted alongside a threat/risk assessment, which is one of the inputs into assessing the overall privacy landscape.

A PIA has at least two roles: one is assisting in privacy compliance, but the other, which has greater meaning for participants not directly responsible for privacy, is building and communicating the information governance and risk management program of the company, including the *PbD* principles. This helps employees at all levels of the organization to better understand the value of the review, its relevance to their job function, and the role it plays in adding value to the organization.

PIAs are already in use in many jurisdictions and different organizational environments, in both the public and private sectors. Recently, for example, the European Commission recommended the use of privacy risk assessments in connection with RFID tags.[39]

With the exception of the *PbD*-PIA currently in development,[40] PIAs are not generally grounded in the 7 Foundational Principles of *Privacy by Design*. Further work in this area is needed.

38 See, for example, Information and Privacy Commissioner/Ontario, The Privacy Diagnostic Tool (PDT) Workbook (Aug 2001), and The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation (Feb 2009), www.ipc.on.ca.

39 European Commission, Commission Recommendation of 12.5.2009 on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification. SEC(2009) 585, SEC(2009) 586, p. 6. http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf).

40 Consistent with the PbD Principles, the forthcoming PbD-PIA will analyze an organization's privacy posture beyond what is required for compliance with laws and regulations. For example, the PbD-PIA will include a comprehensive assessment of the governance of, and accountability for, personal or personal health information collected, used, disclosed, retained and shared, as the case may be. See www.privacybydesign.ca.

Privacy Risk Management

Like other business risks, those related to the protection of personal information benefit from the scrutiny of a formal risk management discipline.

Privacy, and the 7 Foundational Principles of *Privacy by Design*, may be productively incorporated into risk management processes and tools, resulting in the blended discipline of Privacy Risk Management (PRM). Successful PRM depends upon an organization's approach to both the privacy and risk management disciplines.

Organizations with moderate to advanced privacy and risk management capabilities are poised to begin to practice Privacy Risk Management. By embedding privacy into their existing risk management framework, they will be able to manage risks associated with the protection of personal information, in much the same way as any other business risk. Utilizing PRM, performance and value will be enhanced through the execution of proactive processes, rather than ad hoc efforts.

There is a role in PRM for Privacy Risk Management Practitioners. These are much more than simply "Process Custodians." They are also "Agents of Change" – advancing the banner of privacy within an organization, in general, and the risk management function, in particular. While they are critical in ensuring efficient PRM operations, the role itself is one that can be fulfilled by management associated with any of several different functions, depending on the organizational structure. To be truly successful, however, they will require executive visibility and support.

Audits, Seals, and Certification Programs

External validation of an organization's privacy practices can help to ensure the rigor of those practices, identify and address the gaps, help prioritize resources, and contribute to consumer confidence and trust. They can function as a useful source of transparency.

They can also, when appropriately designed, serve as a mechanism for assessing compliance with the principles of *Privacy by Design*, including the extent to which appropriate processes and tools are in place, and are being leveraged, to support a full-fledged organizational commitment to privacy.

When audits or audit-type processes are combined with a seal or certification program that uses a readily recognizable emblem, they can be especially effective in supporting consumer trust objectives.

There are already several privacy seal and certification programs in existence. In the American context, these include TRUSTe, WebTrust, and BBBOnLine.[41] Similar programs exist in other jurisdictions, including Europe's *Europrise* Privacy Seal and Japan's *PrivacyMark*.

Such programs could be expanded or modeled to include considerations linked to the 7 Foundational Principles of *PbD*.

41 From the US Chamber of Commerce web site, http://www.uschamber.com/issues/technology/online-privacy-seal-programs

Regulatory Approaches to *PbD*

Regulatory approaches, for our purposes here, may include certain forms of self-regulation, sectoral privacy laws, omnibus privacy legislation, and, of course, privacy provisions contained in more general laws.

Regulatory approaches to *PbD* throw into sharp relief the ways in which *PbD* invites – and perhaps even requires – innovative new approaches to privacy rule-making. Demand for such innovation is already growing. The European Commission has begun to suggest, for example, that the first generation of privacy legislation, based on Fair Information Practices, has not provided enough guidance, or gone far enough to protect consumers.[42] The Commission is calling for more innovation in the area of privacy regulation.

Scholar Dennis Hirsch suggests that there are valuable lessons to be gleaned for privacy regulators from looking at the history of environmental protection laws, which he characterizes as having been "at the epicenter of an intense and productive debate about the most effective way to regulate" for the past 40 years.[43]

Distinguishing between early "command-and-control" regulatory models, where regulators both commanded the level of required performance and controlled the means of achieving it, and "second generation" approaches, Hirsch points to the success of "[s]econd generation initiatives [that] encourage the regulated parties themselves to choose the means by which they will achieve environmental performance goals… This difference tends to make second generation strategies more cost-effective and adaptable than command-and-control rules."[44]

He suggests that second generation strategies are well suited to information economy industries, which experience rapid change, face stiff competition, and are based on innovation that has the potential to be socially beneficial.

Hirsch's approach is consistent with the findings of the excellent empirical work done by Bamberger and Mulligan, which suggest that, while the dominant theme in U.S. discussions of privacy has suggested a greater need for uniformity and specificity in privacy law, there are advantages offered by also governing privacy through a flexible, principled approach. "While bolstered procedural mechanisms for enhancing informational self-determination may be needed, pursuing that goal in a way that eclipses broader normatively-grounded protections, or constrains the regulatory flexibility that permits their evolution, may destroy important tools for overcoming corporate over-reaching, consumer manipulation, and the collection action problems raised by ceding privacy protection exclusively to the realm of individual choice."[45]

---

42 European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union. (2010) http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

43 See Dennis D. Hirsch, Protecting the Inner Environment: What Privacy Regulation Can Learn From Environmental Law, 41 Georgia Law Review. 1, 8 (2006). http://www.law.capital.edu/faculty/bios/Hirsch%20privacy%20article.pdf, p. 8. This links in interesting ways to parallels drawn between privacy violations and pollution in Ann Cavoukian, A Discussion Paper on
Privacy Externalities, Security Breach Notification and the Role of Independent Oversight. (November 2009). http://www.ipc.on.ca/images/Resources/privacy_externalities.pdf

44 Ibid

45 Bamberger and Mulligan, p. 108.

There is a sound basis for the view that *PbD* lends itself most readily to a flexible, innovation-driven "second generation" approach to regulation; an approach that requires and inspires a common principled commitment to protecting privacy without "imposing intrusive and costly regulation on the emerging business sectors of the information economy."[46]

In our view, the principles of *PbD*, which are described in accessible, non-legalistic language, could be used as the foundation for a second generation approach to privacy regulation. See Appendix B for an example of what such a legal framework could look like.

Precedent certainly exists for incorporating a set of flexible privacy principles into a legislative framework. In Canada, personal information is protected under the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), which applies to the personal information collected, used or disclosed by organizations engaged in commercial activities, from banks and retail outlets to airlines, communications companies and law firms.[47] *PIPEDA* has been fully in force since 2004, and applies to big and small private enterprises across Canada, with the exception of those operating within British Columbia, Alberta and Quebec, where similar provincial statutes exist.[48]

In Canada, as elsewhere, private sector privacy regulation recognizes the dual purposes of protecting the individual's right to privacy on the one hand, and recognizing the commercial need for access to personal information on the other. *PIPEDA* furthers these two purposes by tying a set of flexible, technology-neutral privacy principles to a statutory framework of rules governing the collection, use, and disclosure of personal information.

Part I of the *Act* is drafted using a standard approach to legislation. Schedule I, however, was borrowed from the Canadian Standards Association's *Model Code for the Protection of Personal Information* (Q830), and so does not follow any legislative convention. To accomplish the dual purposes that animate *PIPEDA* and the privacy principles set out in its Schedule, Canada's Federal Court of Appeal has directed that the interpretation and application of this regulatory framework should be guided by "flexibility, common sense and pragmatism."[49]

Developing a *Privacy by Design* regulatory framework would also require an approach guided by "flexibility, common sense and pragmatism." Consider, for example, applying *Privacy by Design* requirements in the context of the Do Not Track discussion, where design solutions must respect the Privacy by Default principle and the Full Functionality – Positive-Sum principle:

> *Scenario: Applying PbD to Do Not Track*
>
> *Privacy by Design* rests on the 7 Foundational Principles, of which Privacy as the Default Setting is the second. Conceptually, this principle requires that personal data be automatically protected. Individuals should not be required to take additional steps to protect their privacy – it should be built into the system, ideally by default. Recently, questions have arisen as to how this principle might be applied in the context of "Do Not Track," which is inherently "opt-out."

46 Hirsch, p. 9, 34-36

47 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.), http://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html.

48 Office of the Privacy Commissioner of Canada, Your Guide to PIPEDA. http://www.priv.gc.ca/information/02_05_d_08_e.cfm

49 Englander v. Telus Communications Inc., 2004 FCA 387, Locus Para. 38-46.

In *Privacy by Design*, Privacy as the Default is the ideal condition to strive for. However, currently, the industry standard of practice for online consumer marketing is opt-out. Privacy as the Default would require a shift to "opt-in." But an immediate shift to an opt-in model (which is the standard of practice for sensitive information, such as personal health information) could be both impractical and, perhaps, harmful to industry.

As one of the 7 Foundational Principles, Privacy as the Default must be read alongside the remaining principles. The fourth principle of Full Functionality (Positive-Sum, not Zero-Sum), requires that *PbD* achieve a doubly-enabling, "positive-sum" solution that provides a win-win result for both consumers and businesses – not one at the expense of the other.

Taking into account the context involved – and context is key – it is possible to develop a two-step process for achieving the spirit of Privacy as the Default in situations where the existing industry standard of practice presents a barrier to achieving the principle directly, right from the outset.

In limited circumstances, where the existing industry standard of practice is opt-out, this Two-Step process may be followed as an interim step towards achieving privacy as the default condition:[50]

- Step 1: Present a clear and "in process" option (i.e. in the course of normal use and operation) for the consumer to opt-out of subsequent online tracking and marketing communications.
- Step 2: Once an individual has chosen to "opt-out" of future tracking or receipt of marketing information, then their choice must remain persistent over time and be global in nature (with respect to that organization).

This two-step process achieves a defacto default condition, in a manner that recognizes legitimate business practices as reflected in industry standards, but is driven by the consumer, and is persistent in its effect – positive-sum, not zero-sum.

Maintaining flexibility with regard to how outcomes and objectives may be achieved is consistent with Hirsch's concept of "second generation" regulatory approaches, and may prove beneficial in promoting and animating meaningful privacy protections. *Privacy by Design*, with its emphasis on positive-sum outcomes, full lifecycle protection, and a flexible implementation model that leverages an organization's capacity to take the lead in identifying the most effective and dynamic way to implement *PbD* in the relevant context, has much to offer in the area of regulatory innovation.

Safe Harbor Initiatives

Regulators and policy-makers may also wish to consider the ways in which approaches to regulating *PbD* may include a possible role for safe harbor initiatives. A safe harbor is a provision of a statute

50 Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, "Do Not Track" Meets Privacy by Design: Announcing a New Two-Step Process for Getting to Privacy as the Default. (Jan. 27, 2011) http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/01/27/do-not-track-meets-privacy-by-design-announcing-a-new-two-step-process-for-getting-to-privacy-as-the-default.aspx

or a regulation that reduces or eliminates a party's liability under the law, on the condition that the party performed its actions in good faith or in compliance with defined standards. These standards may themselves be defined in regulation, legislation, or through standards-making bodies, including industry bodies.

The safe harbor approach has already been used to address privacy-related trade issues between the United States and the European Union. The U.S.-EU Safe Harbor offers a streamlined process for U.S. companies to comply with EU Directive 95/46/EC on the Protection of Personal Data.[51] U.S. companies can opt into the program as long as they adhere to the 7 Fair Information Principles outlined in the Directive.[52]

Similar approaches can also be used by regulators to motivate the adoption of other desirable privacy practices, including *Privacy by Design*. This could encourage organizations to develop and maintain privacy policies as a way of lowering their compliance risks, and motivate them to take due care in embedding privacy protection, at the outset.[53]

Self-Regulation: Voluntary or Government-Mandated Approaches

Traditionally, industry self-regulation and government regulation have been seen as polar opposites. Increasingly, however, they are no longer seen as necessarily mutually exclusive. "As a number of environmental law scholars have observed, self-regulation is a 'highly malleable term which may encompass a wider variety of instruments.' Thus, it is better to think of voluntary self-regulation and direct government regulation as opposing ends of a regulatory continuum, with most regulatory schemes falling somewhere in the middle," in a broad category that can be understood as "mandated" self-regulation.[54]

Joseph Rees distinguishes between two types of mandated self-regulation: full and partial. "Full mandated self-regulation privatizes both of the major regulatory functions of rule making and enforcement. The strategy resembles voluntary self-regulation in this respect, but differs from it chiefly in that a government agency officially sanctions and monitors the self-regulatory program to ensure its effectiveness. In contrast, mandated partial self-regulation limits privatization to one or the other regulatory function, but not both. Two basic approaches are the result: 'public enforcement of privately written rules, and governmentally monitored internal enforcement of publicly written rules.'"[55]

Voluntary codes are already a well-established vehicle in the privacy arena. There are a great many examples of these, worldwide. In March 2011, for example, Germany's digital industry submitted a voluntary code of privacy to the country's government.[56] In Canada, the Investment Industry

51 U.S.-E.U. Safe Harbor Framework, http://www.export.gov/safeharbor/eu/index.asp.

52 After opting in, an organization must re-certify every 12 months. It can either perform a self-assessment to verify that it complies with these principles, or hire a third-party to perform the assessment. There are also requirements for ensuring that appropriate employee training and an effective dispute mechanism are in place.

53 Department of Commerce, Green Paper. p.43.

54 Ira Rubenstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes. NYU School of Law, Public Law Research Paper No. 10-16. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275, p. 3.

55 Joseph V. Rees, Reforming the Workplace: A Study of Self-Regulation in Occupational Safety, 9 (1988), as cited in Rubenstein, p. 12.

56 http://www.monstersandcritics.com/news/europe/news/article_1622883.php/German-geodata-industry-submits-voluntary-code-of-privacy-to-Berlin

Regulatory Organization of Canada developed a Privacy Code that binds its members.[57] In New Zealand, there are privacy Codes of Practice in the areas of health, telecommunications, and credit reporting.[58] In the U.S., voluntary codes are well-established, and have been the subject of several reports to Congress.[59]

Activity in this area continues. For example, promising steps have been made toward the development of a voluntary code for online behavioral advertising in the United States.[60] Although still in its early stages (as this paper was being written), essential features of this code would include publicly acknowledged adherence to basic guidelines, compliance assessments, complaint mechanisms, self-policing measures, and periodic updates.[61]

The process involved in arriving at voluntary or self-regulatory codes can produce significant benefits in and of itself. Generally, this process involves a trade association or group of firms establishing substantive rules concerning the collection, use and transfer of personal information and procedures for applying these rules to member firms.[62] "Self-regulatory guidelines require that firms come together and engage in a deliberate and normative discussion of the principles that should guide their activities with respect to a public policy goal such as privacy protection. This inevitably involves candid reflections on how a company should handle information processing challenges both in terms of its own business model and as compared to other firms in the industry." Thus, the very act of participating in the drafting of self-regulatory principles provides company representatives with a highly relevant basis for questioning how their own firms do business. At the same time, achieving consensus as to industry principles lays the foundation for future compliance by forming an "expectation of obedience." Legal norms contribute to this expectation since agreement to industry principles creates legally enforceable obligations."[63]

In an evolving area such as privacy, the multi-stakeholder process of establishing norms can present an important opportunity to gauge consumer expectations and align business practices with them more effectively.

Voluntary codes are not without their challenges. To the extent that voluntary codes of practice are either not mandated or only weakly mandated by government, for example, they can raise concerns about "free riders." The free rider problem may manifest itself in one of two ways: "[F]irst, some firms may agree to join a program but merely feign compliance; second, certain firms in the relevant sector may simply refuse to join at all."[64] Nonetheless, they represent an important vehicle that serves a useful purpose.

57 http://www.iiroc.ca/English/About/Governance/Documents/PrivacyCode_en.pdf
58 http://privacy.org.nz/the-privacy-act-and-codes/
59 See, for example, FTC, Self-Regulation and Privacy Online: Report to Congress 6 (1999), http://www.ftc.gov/os/1999/07/privacy99.pdf
60 Department of Commerce, Green Paper, p. 42. More work remains to be done in this area, however. FTC Commissioner Jon Leibowitz has publicly criticized Google for its reluctance to voluntarily adopt privacy measures like "Do Not Track," See Mike Zapler, Jon Leibowitz: Google Should Step up on Privacy, Politico (Apr. 19, 2011, 6:45 PM EDT), http://www.politico.com/news/stories/0411/53440.html. In addition, Commissioner Leibowitz acknowledged that it is unclear how many online advertisers would be willing to honor voluntary measures like "Do Not Track."
61 Department of Commerce, Green Paper, p. 42.
62 Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes. New York University School of Law Public Law & Legal Theory Research Paper Series, Working Paper No. 10-16. (March 2010). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275, p 2.
63 Ibid, p. 28.
64 Ibid, p. 24.

Sectoral Laws

Sector-specific legislation has arguably been the dominant method for setting privacy policy in the United States.[65] There are countless sectoral laws that pertain wholly or partially to the protection of personal information at the state and federal levels.[66]

Critics suggest that sector-specific legislation creates a patchwork of laws, sometimes with overlapping application, some of which may be in conflict, creating uncertainty for businesses and consumers alike. But this view is not uniformly held, and it has also been suggested that sectoral laws provide an important avenue for experimentation in the privacy arena.[67]

One area where sector-specific privacy regulation may be particularly useful is with regard to industries or practices that are in their nascent stages, where standards for the protection of personal information can be set early on, and then be more easily absorbed as part of the initial architecture. A good example of such a scenario is the emerging Smart Grid.[68]

The Smart Grid, which is viewed as essential to the future provision and conservation of energy, will drive an increase in the amount of digitized information gathered relating to consumer activities within their homes. In many cases, the infrastructure will be capable of informing consumers' hourly and real-time energy use, right down to the appliance level.

In Ontario, Canada, as in other jurisdictions, the Smart Grid is beginning to develop through the widespread installation of smart meters, time-of-use, demand management initiatives, and the creation of a Smart Metering Entity resulting from legislative action by the Government of Ontario in the *Green Energy Act, 2009* and the *Electricity Act, 1998*. The province's goal is to meet electricity demand over the next 20 years, while also achieving energy conservation and use of renewable energy resources (for example, to discontinue the use of coal plants by 2014).

Functional specifications were issued by the government that all electricity providers must meet in achieving smart meter policy goals to support the Smart Grid, with the Smart Metering Entity being responsible for the consolidation, management and storage of consumer electricity consumption information.[69]

Electricity distributors in Ontario are required to adhere to these functional specifications when installing smart meters, metering equipment, systems and technology. They are also required to meet all applicable federal, provincial and municipal laws, codes, rules, directions, guidelines, regulations and statutes, including requirements of regulatory authorities and agencies such as the Canadian Standards Association and Measurement Canada.

---

65 Department of Commerce, Green Paper. p. 11.

66 See, for example, http://www.privacy.ca.gov/privacy_laws.htm

67 Paul M. Schwartz, Preemption and Privacy. The Yale Law Journal. 118:902 2009 http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/preemption_and_privacy.pdf

68 Information and Privacy Commissioner/Ontario, Hydro One, & Toronto Hydro, Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid. (June 2010) http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf p. 1-2.

69 A Ministerial Directive issued by the Minister of Energy on November 23, 2010 requires that, in performing its functions, the OEB be guided by several government policy objectives including the following: "Privacy: Respect and protect the privacy of customers. Integrate privacy requirements into smart grid planning and design from an early stage, including the completion of privacy impact assessments."

In order to meet their privacy obligations, and to help build the consumer confidence and trust that is essential to the full implementation of the Smart Grid, Ontario utilities have implemented a *Privacy by Design* approach, with tremendous success.[70] In February 2011, the Ontario Information and Privacy Commissioner, along with Hydro One, GE, IBM and Telvent, issued a guidance document based on implementing *PbD* in a cutting-edge Smart Grid project in Owen Sound in Ontario, Canada. The paper demonstrates how the principles of *Privacy by Design* may be operationalized as a foundational requirement in emerging Smart Grid systems, setting the precedent for other utilities to follow.[71]

The National Institute of Standards and Technology (NIST) has also recommended *PbD* as a methodology for future Smart Grid development,[72] as has the European Commission's Task Force on Smart Grids.[73] "Privacy should be designed into smart meter systems right from the start as part of the compliance life-cycle and include easy to use privacy-enhancing technologies. We urge to make the principle of privacy by design mandatory, including principles of data minimization and data deleting."[74]

Omnibus Privacy Legislation

Omnibus privacy legislation provides a vehicle for describing a desired end state in terms of how personal information is managed and protected. The principles of *Privacy by Design* can inform both the end state (e.g. privacy as the default), and the process for arriving at the end state (e.g. end-to-end, full lifecycle protection).

While *PIPEDA* and the substantially similar provincial statutes do not reference *PbD* specifically, the principles of *Privacy by Design* may come into play where privacy investigations have identified gaps in an organization's practices, as outlined later in this paper.

In the U.S., omnibus privacy legislation does not exist, though it has been hotly debated for several years.[75] Without getting into the pros and cons of such legislation, it is clear that omnibus legislation would provide a solid vehicle for enshrining the principles of *Privacy by Design*. There is already movement in this direction: in 2011, Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the *Commercial Privacy Bill of Rights*[76] that would require businesses that collect, use, store or transfer consumer information to implement a *Privacy by Design* approach when developing

70 *Ibid*, plus 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

71 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

72 The Smart Grid Interoperability Panel–Cyber Security Working Group, Department of Commerce and National Institute of Standards and Technology, NISTIR 7628: Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

73 Task Force Smart Grids, Expert Group 2: Regulatory Recommendations for Data Safety, Data Handling and Data Protection (February 16, 2011). http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

74 European Association for Co-orindation of Consumer Representation in Standardisation (ANEC), http://www.anec.org/attachments/ANEC-PT-2010-AHSMG-005final.pdf

75 The history of this debate is long and interesting. See Schwartz for an abbreviated version of it.

76 John Kerry, Commercial Privacy Bill of Rights. http://kerry.senate.gov/work/issues/issue/?id=74638d00-002c-4f5e-9709-1cb51c6759e6&CFID=90056053&CFTOKEN=63781113

products and provide consumers with choices about how data are used, collected and shared.[77] This is the first time that *Privacy by Design* has been explicitly included in a bill.

Enforcement and Remedial Approaches to *PbD*

Regulatory approaches to privacy protection may include not only sector-specific laws that wholly or partially relate to privacy, or omnibus privacy legislation, but also provisions under the general civil or criminal law. Particularly in the case of the latter two, *PbD* may also be promoted through creative approaches to enforcement, sentencing, and negotiated settlements.[78]

Alternatively, governments may wish to use evolving jurisprudence in connection with existing legislation. For example, it has been suggested that privacy in the United States be viewed as a dimension of non-price competition, which would make it a cognizable interest under U.S. antitrust laws.[79] Similarly, the FTC's authority under Section 5 of the FTC Act has been used to remedy corporate infringement of privacy rights successfully.[80] The FTC and the Department of Commerce have worked together with both commercial and non-commercial stakeholders to develop models for addressing privacy challenges posed by emerging technologies, as they develop.[81]

There is a growing understanding that even organizations that are in full compliance with privacy laws – particularly those based on FIPs – can find themselves embroiled in controversy because they are out of step with consumer *expectations* about how personal information should be handled. Consumers, increasingly, are experiencing what they consider to be "privacy harms" even where there has been no technical violation of a privacy statute. This reflects, in part, the fact that detailed legal frameworks are often slow to respond to fast-paced innovative technologies and practices. But it also reflects a particular set of assumptions about the nature of privacy harm that may need to evolve in today's online world.

77 Section 103 of the *Kerry-McCain Commercial Privacy Bill of Rights Act of 2011* (CPBR) provides that:
Each *covered entity* [defined term] shall, in a manner proportional to the size, type, and nature of the *covered information* [defined term] that it collects, implement a comprehensive information privacy program by —
(1) incorporating necessary development processes and practices throughout the product lifecycle that are designed to safeguard the *personally identifiable information* [defined term] that is *covered information* of individuals based on—
(A) the reasonable expectations of such individuals regarding privacy; and
(B) the relevant threats that need to be guarded against in meeting those expectations; and
(2) maintaining appropriate management processes and practices throughout the data lifecycle that are designed to ensure that information systems comply with—
(A) the provisions of this Act;
(B) the privacy policies of a *covered entity*; and
(C) the privacy preferences of individuals that are consistent with the consent choices and related mechanisms of individual participation as described in section 202 [right to notice provisions]. [Emphasis added.]

78 I am deeply grateful to Pamela Jones Harbour for her insights in this regard.

79 Pamela Jones Harbour & Tara Isa Koslov, Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets, 76 ANTITRUST L. J. 769, 773 (2010)

80 Federal Trade Commission, Staff Report, p. 12-13. See Section III(A)(2)(e), infra, for examples of the FTC's recent use of its remedial powers in the privacy arena.

81 Department of Commerce, Green Paper, p.19-20.

In *The Boundaries of Privacy Harm*, M. Ryan Calo[82] argues that privacy harm is a unique injury with specific boundaries and characteristics.[83] He suggests that these fall into two related categories: *subjective* privacy harm, which is the perception of unwanted observation, and *objective* privacy harm, which is the unanticipated or coerced use of information about an individual, with adverse consequences to the individual. These two components of privacy harm are two sides of the same coin – the loss of control over information about oneself, in effect, the opposite of informational self-determination.[84]

A most interesting aspect of Calo's work is the way in which, by the uncoupling of privacy harms from privacy violations, may permit the measurement and redress of privacy harm in novel ways.

To what extent does this uncoupling invite a creative revisiting of our approach to preventing and remedying privacy harms? For example, where there has been, or is a risk of, a subjective privacy harm, consider that there will typically be an increased risk of objective privacy harm. Going forward, *PbD* has the potential to proactively and responsively address both types of harm. Where *PbD* has not been applied proactively, decision-makers can impose terms and conditions that fulfill an organization's *PbD* responsibilities remedially. This can serve to remedy privacy harms by ensuring that:

- Privacy is "baked in" as a resourced corporate priority, addressing the full information lifecycle;
- The unwanted observation of personal information is minimized;
- Necessary observations are broadly understood as serving legitimate and well-defined purposes;
- The organization's information handling practices are visible transparent; and
- Customers are able to exercise choices regarding their participation in data-related practices.

One example of the possible application of this approach is with the FTC. The FTC has the ability to issue orders compelling companies to remediate unfair practices or antitrust violations and has previously imposed consumer privacy-related terms in their consent decrees. In 2002, the FTC alleged that Eli Lilly and Company had not adequately safeguarded consumer information that had been submitted on the company's website.[85] To resolve the charges, the company agreed to appoint a Chief Privacy Officer and implement a privacy protection program.[86] Among the features of that program were the assessment of privacy risks, periodic monitoring and ongoing evaluation efforts.[87]

This approach has also been used by Canada's Privacy Commissioner in her role as overseer of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). During her investigation of Google's Street View map service, Google acknowledged that it had inadvertently collected data

82 M. Ryan Calo, The Boundaries of Privacy Harm. 86 Indiana Law Journal (Summer 2011) pgs 1, 12-13.
83 This in contrast, for example, to Daniel Solove's approach, which rejects the idea that privacy can or should be reduced to one or even multiple concepts. Any boundaries put around the idea of privacy or privacy harm ends up including some activities that do not deserve the label "privacy" and excluding others that do. Instead, Solove creates a taxonomy of privacy rights and interests consisting of matters that do no all have one thing in common. See Daniel J. Solove, A Taxonomy of Privacy. 154 U. Pa. L. Rev. 477, 482 (2006).
84 The German concept of "informational self-determination" was first used in the context of a German constitutional ruling relating to personal information collected during the 1983 census.
85 Eli Lilly and Company, FTC Docket No. C-4047, Compl. 10 (2002), http://www.ftc.gov/os/ 2002/05/elililllycmp.htm.
86 Eli Lilly and Company, FTC Docket No. C-4047, Order. 2 (2002), http://www.ftc.gov/os/ 2002/05/elililllydo.htm.
87 *Ibid*.

transmitted over unprotected wireless networks installed in homes and businesses in Canada (and around the globe). The report concluded that the incident had largely resulted from Google's lack of proper privacy policies and procedures.

After the Privacy Commissioner issued her findings and recommendations in October 2010, Google agreed to implement key privacy by design-related recommendations, including:

- Implementing a system for tracking all projects that collect, use or store personal information and holding the engineers and managers responsible for those projects accountable for privacy;
- Requiring engineering project leaders to draft, maintain, submit and update Privacy Design Documents for all projects in order to help ensure that engineering and product teams assess the privacy impact of their products and services, from inception through to launch;
- Assigning an internal audit team to conduct periodic audits to verify the completion of selected Privacy Design Documents, and their review by the appropriate managers; and
- Piloting a review process whereby members of Google's Privacy Engineering, Product Counsel and Privacy Counsel teams review proposals involving location-based data, as well as the software programs that are to be used for the collection of data.[88]

While there is no question that tackling privacy issues up front, and embedding privacy protections directly into new systems, processes, and architectures, is optimal from both a privacy and a business perspective, the reality is that it is not always possible to embed privacy directly from the outset. Most organizations operate in the context of existing, relatively mature IT systems and business practices, which they have developed and evolved over time, as business or other needs have dictated. Remedial measures such as the ones outlined above demonstrate the relevance of *Privacy by Design*, even in these circumstances.

An extension of *PbD*, *Privacy by ReDesign* is used to describe a new approach to applying the 7 Foundational Principles of *Privacy by Design* to legacy systems and existing operations. Clearly, since existing systems are already operational and pervasive throughout most organizations, the principles cannot be embedded right from the outset. Instead, the objective must be to approach the end state of *PbD* – the highest standard of privacy protection – by seizing opportunities to Rethink, Redesign, and Revive these systems.[89]

88 Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2011-001. June 6, 2011. http://www.priv.gc.ca/cf-dc/2011/2011_001_0520_e.cfm. Also see TJX Companies Inc./Winners Merchant International L.P., [2007] A.I.P.C.D. No. 34, a joint investigation of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of Alberta. The case arose in relation to concerns about a network computer intrusion affecting the personal information of an estimated 45 million payment cards in Canada, the United States, and elsewhere. Following their investigation, the Commissioners recommended and the organizations agreed to dedicate "significant resources to enhance the security of its systems, including the monitoring of its systems" and adopt more robust encryption technology.

89 Ann Cavoukian and Marilyn Prosch, Privacy by ReDesign: Building a Better Legacy. (May 2011) http://privacybydesign.ca/content/uploads/2010/03/PbRD.pdf

Conclusion

There is a clear appetite for mechanisms that support meaningful privacy protection while also enabling flexibility and innovation. *Privacy by Design*, with its emphasis on doubly-enabling, positive-sum outcomes, is rapidly emerging as the gold standard in privacy and data protection. It offers decision-makers the opportunity to develop principled and pragmatic solutions that leverage the *PbD* advantage.

PbD represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches, bolted on after the fact. Enshrining *PbD* in policy, regulatory instruments, voluntary codes, and best practices requires an evolution in how policy and law makers approach privacy rule-making.

PbD's flexible, innovation-driven approach to achieving privacy can help to encourage organizations to "internalize the goal of privacy protection and to come up with ways to achieve it. This approach could be advanced, for example, as part of a second generation regulatory framework. In the complex, fast-moving information economy, this strategy could be an effective way to enhance privacy protection."[90]

Under the influence of such a "second generation" approach, incorporating the principles of *Privacy by Design*, companies can be encouraged to "go beyond mere legal compliance with notice, choice, access, security and enforcement requirements."[91] Instead, they can be empowered to design their own responsive approaches to risk management and privacy-related innovation, within the context of a policy or regulatory framework.

Some industry leaders are already moving towards implementing *Privacy by Design* within their organizations as a way of actualizing their commitment to privacy, while aligning more closely to consumer expectations. Policy discussions in the U.S., the EU, and elsewhere have begun to include consideration of *PbD* as a necessary component of future approaches to protecting privacy. Momentum behind *PbD* as the next generation of privacy protection is growing strong.

This paper has outlined a variety of vehicles that are available to legislators and policy-makers to help support the widespread implementation of the principles of *Privacy by Design*. It is our hope that this paper will serve to stimulate dialogue and innovation within the privacy arena, supporting meaningful privacy protection, now and well into the future.

90 Hirsch, p. 63
91 Rubinstein, p. 52

Appendix A:
The 7 Foundational Principles of *Privacy by Design*[92]

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

The *Privacy by Design* (*PbD*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. ***Full*** Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

92 Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, *The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*, http://www.privacybydesign.ca/content/uploads/2010/05/pbd-implement-7found-principles.pdf.

6. Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy

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

Appendix B:
What *PbD* Could Look Like as Part of a Legal Framework

This draft legal framework is offered to stimulate discussion on how to provide a flexible but enforceable legal framework for PbD, for example as part of a safe harbor initiative or an omnibus privacy statute. It draws on Commissioner Cavoukian's 7 Foundational Principles: Implementation and Mapping of Fair Information Practices http://www.privacybydesign.ca/content/uploads/2010/05/pbd-implement-7found-principles.pdf; the Privacy Commissioner of Canada's Google report, PIPEDA Case Summary #2011-001; Section 103 of the Kerry-McCain Commercial Privacy Bill of Rights Act of 2011; and elements of the Massachusetts Data Breach Notification Law and Massachusetts Executive Order 504.

> Each organization shall, in a manner proportional to the organization's size, scope, and resources and the size, type, and nature of the *personal information* that it collects, implement a comprehensive *Privacy by Design* program by:
>
> (1) Incorporating necessary development processes and practices designed to safeguard the *personal information* of individuals throughout the lifecycle of a product, program or service and
>
> (2) Maintaining appropriate management processes and practices throughout the data lifecycle that are designed to ensure that information systems comply with:
>
> (A) Privacy requirements provided for by law;
>
> (B) The privacy policies of the *organization*; and
>
> (C) The privacy preferences of individuals that are consistent with the applicable mechanisms required or provided to give effect to individual choice.

A comprehensive *Privacy by Design* program must include the following elements:

(1) An organization shall establish a *Privacy by Design* leader and/or team by identifying the appropriate directors, officers, and managers responsible for developing, maintaining, implementing, and updating proactive *Privacy by Design* processes and practices;

(2) Proactive *Privacy by Design* processes and practices shall:

(A) Apply to the design and architecture of infrastructure, IT systems, and business practices that interact with or involve the use of any personal information;

(B) Describe each of the core purposes served and main functions delivered by those infrastructures, systems and practices, including but not limited to the provision of security and the protection of privacy in personal information;

(C) Incorporate data minimization and provide the highest degree of privacy protection for personal information possible while serving the other core purposes and delivering the other main functions;

(D) Provide this degree of privacy protection by employing the maximum feasible means needed to ensure the security, confidentiality, and integrity of personal information throughout the lifecycle of the data, from its original collection, through to its use, storage, dissemination, and secure destruction at the end of the lifecycle;

(E) Whenever reasonably possible, provide for that privacy protection automatically, so that no action is required for individual users or customers to protect the privacy of their personal information;

(F) Ensure that infrastructure, IT systems, and business practices that interact with or involve the use of any personal information remain reasonably transparent and subject to independent verification by all relevant stakeholders, including customers, users, and affiliated organizations; and

(G) Emphasize the design and maintenance of user-centric systems and practices, including strong privacy defaults, appropriate notice, and other user-friendly options.

In support of a comprehensive *Privacy by Design* program, an organization must:

(1) Provide appropriate privacy and security training to its employees;

(2) Implement a system for tracking all projects that regularly collect, use or store personal information;

(3) Require project leaders to draft, maintain, submit and update Privacy Design Documents for all projects in order to help ensure product, program or service teams assess the privacy impact of their products, programs and services from inception through launch; and

(4) Assign an internal audit team to conduct periodic audits to verify the completion of selected Privacy Design Documents and their review by the appropriate managers.

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

August 2011

http://www.privacybydesign.ca

Information and Privacy Commissioner,
Ontario, Canada