Operationalizing *Privacy by Design*:

A Guide to Implementing Strong Privacy Practices

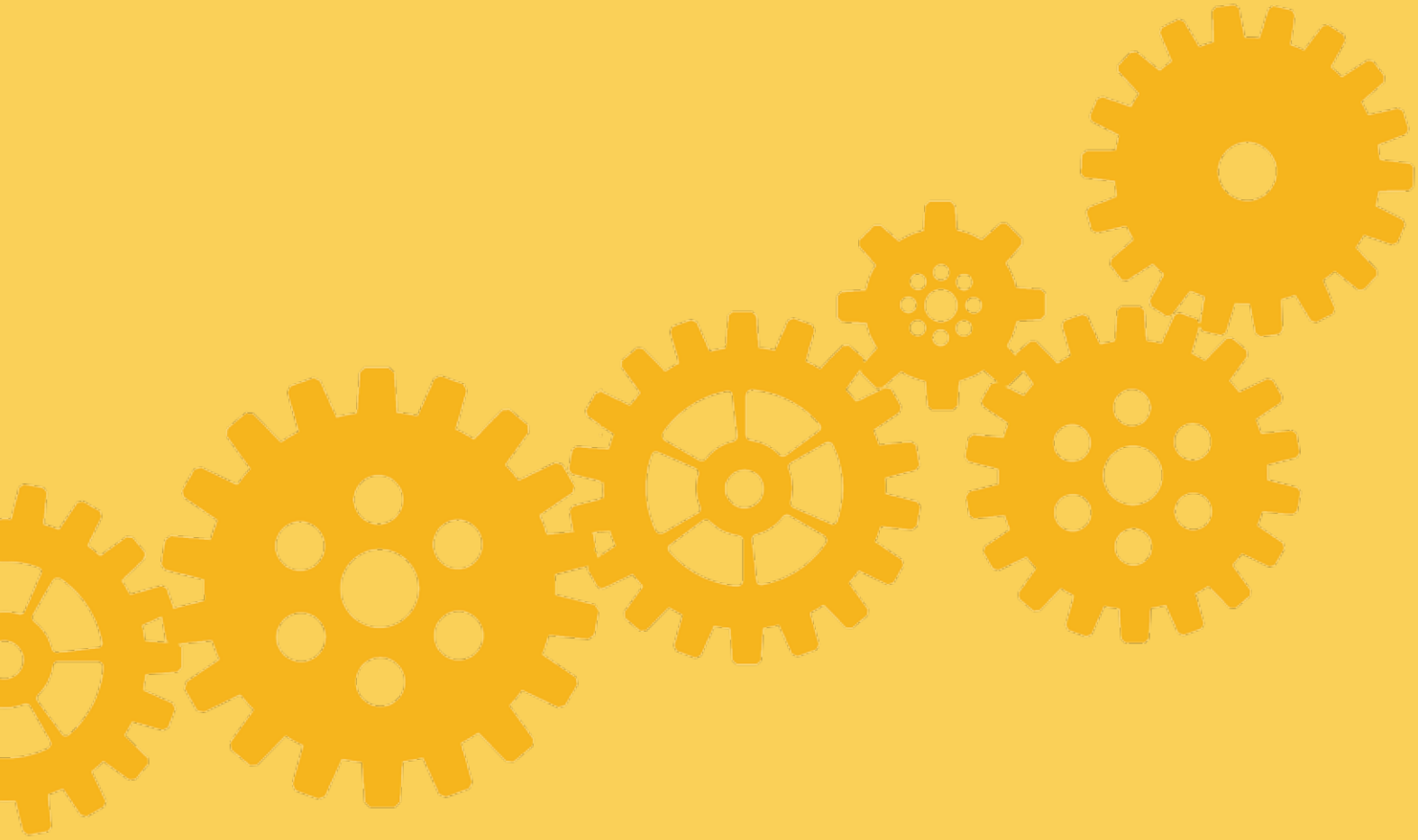
Ann Cavoukian, Ph.D.

Information and Privacy Commissioner,
Ontario, Canada

December 2012

Acknowledgements

A considerable amount of work has gone into this paper and I am grateful to my staff without whom this monumental task couldn't be completed. Special thanks to Ken Anderson, Michelle Chibba, Fred Carter, Estella Cohen, Jeff Kirke and Sandra Kahale for their specific contribution. I also wish to acknowledge the many partners who have joined me as co-authors in the numerous papers written over the last several years, generously lending their expertise to broadening the *PbD* experience.



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

Table of Contents

Executive Summary 1

Introduction 5

The Fundamentals 7

- Privacy: A Practical Definition 7
- The 7 Foundational Principles of *Privacy by Design* 8
- Implementation Guidance 9

The 7 Foundational Principles of *Privacy by Design* 12

- ***Proactive*** not Reactive; ***Preventative*** not Remedial 13
- Privacy as the ***Default Setting*** 21
- Privacy ***Embedded*** into Design 26
- Full Functionality – ***Positive-Sum***, not Zero-Sum 33
- End-to-End Security – ***Full Lifecycle Protection*** 38
- ***Visibility*** and ***Transparency*** – Keep it ***Open*** 44
- ***Respect*** for User Privacy – Keep it ***User-Centric*** 49

Conclusions 54

Appendices 55

Privacy by Design Papers Organized by Application Area 55

CCTV/Surveillance Cameras in Mass Transit Systems: 55

Biometrics Used in Casinos and Gaming Facilities 55

Smart Meters and the Smart Grid 56

Mobile Devices & Communications 56

Near Field Communications (NFC) 57

RFIDs and Sensor Technologies 57

Redesigning IP Geolocation Data 57

Remote Home Health Care 57

Big Data and Data Analytics 58

Foundational *PbD* Papers 58

Privacy by Design Papers Organized by Principle 59

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial 59

2. Privacy as the ***Default Setting*** 60

3. Privacy ***Embedded*** into Design 61

4. Full Functionality – ***Positive-Sum***, not Zero-Sum 62

5. End-to-End Security – ***Full Lifecycle Protection*** 63

6. ***Visibility*** and ***Transparency*** – Keep it ***Open*** 63

7. ***Respect*** for the User – Keep it ***User-Centric*** 64

Executive Summary

It has been almost 20 years since I developed the concept of *Privacy by Design (PbD)*. Reflecting on the widespread acceptance it currently enjoys within the public and private sectors, as well as its endorsement by the International Association of Data Protection Authorities and Privacy Commissioners, the U.S. Federal Trade Commission, the European Union and privacy professionals, is particularly gratifying. While much has been accomplished, much work still remains. The time has come to give deeper expression to *PbD*'s 7 Foundational Principles.

Over the past several years, my Office has produced over 60 *PbD* papers with many well-known subject matter experts ranging from executives, risk managers, legal experts, designers, analysts, software engineers, computer scientists, applications developers in telecommunications, health care, transportation, energy, retail, marketing, and law enforcement.

While some of our papers are "foundational" works, much of our *PbD* research is directly related to one of nine key application areas:

Privacy by Design Application Areas

1. CCTV/Surveillance Cameras in Mass Transit Systems;
2. Biometrics Used in Casinos and Gaming Facilities;
3. Smart Meters and the Smart Grid;
4. Mobile Devices & Communications;
5. Near Field Communications (NFC);
6. RFIDs and Sensor Technologies;
7. Redesigning IP Geolocation Data;
8. Remote Home Health Care;
9. Big Data and Data Analytics.

The good news is that new insights are beginning to emerge – a set of common messages, each associated with the 7 Foundational Principles, has become apparent. This is particularly important because it further validates our initial principles, which are considerably broader in scope and extend well beyond Fair Information Practices. It is these "messages" with which this paper is primarily concerned.

The challenge is that there is no "one-size-fits-all" response to specific "developer-level" privacy requirements. In fact, since the successful implementation of *Privacy by Design* rests on the ***specific privacy requirements*** provided by business and application owners to developers, it seems improbable that a comprehensive canon of privacy requirements will be developed in the near future. However, such a goal is laudable and progress is already underway through the work of a new OASIS Technical Committee dedicated to developing and promoting standards for *PbD* in software engineering. Certainly, as implementation of strong privacy protections within applications becomes more common, I expect that a movement toward shared code libraries will develop, much as developers share code for other commonly required functions.

In this paper, as in many others, I begin by framing privacy as an issue of control – the need to maintain personal control over the collection, use and disclosure of one's personally identifiable information. It is a concept that is best reflected in the German right of "informational self-determination" and that the individual should be the one to determine the fate of his or her personal information. Recognizing privacy as an exercise in control has always been important, but it is critical today in an age characterized by far-reaching online social media and ubiquitous computing.

Too often, issues of privacy and the protection of personal information are regarded as the domain of large corporations – those with a Chief Privacy Officer or formal privacy infrastructure. This is not the case. The Internet has proven to be such a tremendous leveller – today, relatively small organizations may control disproportionately large volumes of PII. Every organization bears a responsibility to understand its relationship with PII and strategize accordingly. I believe that they would all benefit from embracing *PbD*. In this paper, I argue that it is not the size or structure of the organization that matters, what matters is that someone is charged with the responsibility of being accountable for the organization's privacy protection. In a large company, this may be the CPO, supported by application owners and developers; in a smaller one, perhaps the founder is the one to be held accountable, relying on contracted IT resource for support.

PbD, relying on building privacy in – early, robustly and systematically – across the business ecosystem, yields meaningful benefits. Doing it right, the first time, has long been recognized as a cost-saving strategy in multiple domains. Most importantly, however, the approach fosters an environment where privacy harms are minimized or entirely prevented from happening, in the first place. Imagine the cost savings in avoiding data breaches and the duty of care that follows.

Considering each of the 7 Foundational Principles, I describe a collection of associated activities that may be described as "best practices" with respect to the execution or fulfilment of that principle. And, while organizational size and structure present challenges to describing performance accountability, I have suggested typical job titles, or levels of responsibility, where performance of these activities is expected.

In summary, the activities and responsibilities for each of the 7 Foundational Principles include:

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial – The focus is on the role played by organizational leadership/senior management in the formation, execution and measurement of an actionable privacy program. Research and case studies pertaining to the role of Boards of Directors, the definition of an effective privacy policy, the execution of a "*PbD* Privacy Impact Assessment" (a truly holistic approach to privacy and privacy risk management) and a "Federated PIA," as well as a variety of other applications contribute to further implementation guidance.

2. Privacy as the ***Default Setting*** – Focusing on a new group within the organization, we examine the critical role that business and application owners play in the development of privacy requirements – requirements that will be incorporated into processes and technologies developed by software engineers. The importance of minimizing the collection of personal information, purpose specification, use limitation and barriers to data linkages is reinforced. A variety of technologies – IP geolocation, anonymous digital signage, de-identification and biometric encryption – highlight specific innovative solutions to this challenge.

3. Privacy ***Embedded*** into Design – Continuing to focus on staff with responsibility for the delivery of privacy, we consider the role of a Privacy Risk Assessment. Further, we stress the importance of the "Laws of Identity" and the incorporation of privacy in system development lifecycles and the variety of regulatory approaches. Case studies focusing on how privacy is embedded into design include: IBM and their Big Data Sensemaking Engine; San Diego Gas and Electric's incorporation of privacy into their Smart Pricing Program; and, the application of specific privacy design features for the mobile communication ecosystem.

4. Full Functionality – ***Positive-Sum***, not Zero-Sum – *PbD*'s positive-sum approach is at once, one of its most important, yet most challenging dimensions. The essence of *PbD* is that multiple, legitimate business interests must coexist with privacy. The notion that privacy requirements must be traded off against others (e.g. security vs. privacy or performance vs. privacy) is discarded as a dated formulation from the past. Innovative privacy solutions must prevail. Among those who have answered the call are the Ontario Lottery and Gaming Corporation, who have used privacy-protective facial recognition technology to ensure that self-excluded gamblers are kept off-site without compromising the privacy of other patrons. The Toronto Transit Commission have developed an approach to video surveillance that is both comprehensive *and* privacy-protective. Other technologies that we examine include: Electronic Health Records, Home Health-Care Technologies, Smart Meters and the Smart Grid.

5. End-to-End Security – ***Full Lifecycle Protection*** – Security is generally well understood, though occasionally confused by some with privacy. We consider the appropriate implementation of encryption by default, especially on devices susceptible to loss, theft or accidental disposal as well as the secure destruction and disposal of personal information at the end of its lifecycle. Much of our work considers the application of this principle within the health-care sector, but we also discuss its application within Google's Gmail, Cloud computing environments, the Smart Grid and video surveillance.

6. ***Visibility*** *and* ***Transparency*** – Keep it ***Open*** – Visibility and transparency are hallmarks of a strong privacy program – one which inspires trust in an organization. We describe a collection of best practices that render the organization's approach to privacy perfectly clear to its customers, clients or citizens. We also stress the importance of audit trails as an approach to help users understand how their data is stored, protected and accessed.

7. ***Respect*** for the User – Keep it ***User-Centric*** – The privacy interests of the end-user, customer or citizen are paramount. *PbD* demands that application and process developers undertake a collection of activities to ensure that an individual's privacy is protected even if they take no explicit steps to protect it. Privacy defaults are key; clear notice is equally important. Especially within complex systems (e.g. contemporary Social Network Services), users should be provided with a wide range of privacy-empowering options. We consider "Government 2.0" (an application of Web 2.0) and the critical role that User Interface Design plays, as well as the emerging recognition of the value of one's personal information and the rise of the Personal Data Ecosystem. Finally, we consider an intriguing and potentially powerful new form of Artificial Intelligence called SmartData.

This is a lengthy paper – since it consists of the vast body of work previously published by my office. But it is not a summary of those papers. It represents an in-depth review of that work and a systematic consolidation and categorization of their seemingly disparate lessons.

I urge you to read this paper from beginning to end – the scope of the lessons and, more importantly, their holistic interplay will hopefully entice you. Recognizing its length, however, there are other reading strategies one may choose to adopt:

- Using the tables at the beginning of each principle, one can undertake a cursory survey of the lessons and responsibilities associated with each of the 7 Principles.

- Choosing to focus on any single principle, one may dive deeply into our work by reviewing the case studies summarized in each section.

- Those wishing to delve even more deeply, may wish to consult the references identified and illustrated within. Using the electronic version of this paper, clicking on a source or cover illustration will link you back to the original work.

Finally, two rather lengthy appendices are presented. The first, a chronological presentation of our *PbD* work is useful in assessing the evolution of our approach to the topic. The second groups the papers into either the "foundational" category or one of the nine key application areas.

Privacy by Design's value as a privacy framework is now well recognized. There are many organizations that have worked hard to achieve this gold standard for privacy and more continue to implement *PbD* within their organization's processes, applications and offerings. Your work serves the cause of privacy – the protection of our personal information. For this, you have my eternal thanks! Let us continue to work together to ensure that privacy grows strong and prevails, well into the future.

Introduction

Comprehensive privacy programs are an essential component of building trusting, long-term relationships with existing customers and attracting opportunity in the form of new ones. Privacy breaches can have profound and long-term adverse consequences, including significant financial impacts and damage to the brand and reputation of organizations.

The momentum behind *Privacy by Design (PbD)* has been growing for the past several years. Its global acceptance demonstrates that the power of the 'build it in early' approach to privacy is truly without borders. Now, as this concept spreads, the question that remains is, "We believe in *PbD* – but how do we do it?"

We are now at the stage where market and technology leaders, academics and regulators are beginning to look at ways of translating the principles of *PbD* into technical and business requirements, specifications, standards, best practices, and operational performance criteria.[1] Having repeatedly said that *PbD* is not a theoretical construct, its actual application on the ground must be demonstrated.

This paper provides an overview of the partnerships and joint projects that the Office of the Information & Privacy Commissioner of Ontario, Canada (IPC) has been engaged in over the years to operationalize *Privacy by Design* – providing concrete, meaningful operational effect to its principles. Informed by a broad collection of papers, it represents insights from a wide range of sectors, including telecommunications, health care, transportation, and energy. Further, it draws on the perspectives and experiences of executives, risk managers, lawyers and analysts, as well as engineers, designers, computer scientists and application developers, to name a few – all working to pursue privacy based on the principles of *Privacy by Design*. By reflecting on the experiences of others, it is my hope that privacy leaders will recognize an approach for their organizations to follow or be inspired to create one of their own.

I also hope that, like the organizations highlighted here, new players will come forward to share their experiences, lessons learned, and accomplishments, arising through alignment of their organizations and operations with the principles of *Privacy by Design*, so that we may continue to build much-needed expertise, and grow best practices, for the benefit of all.

1 See Viewpoint: Spiekermann, S. (July 2012). The Challenges of *Privacy by Design*. Communications of the ACM, 55, 7, p.38-40; Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering *Privacy by Design*. Computers, Privacy & Data Protection; Kost, M., Freytag, J. C., Kargl, F., & Kung, A. (August 22-26, 2011). Privacy Verification Using Ontologies. Paper presented at the Availability, Reliability and Security (ARES), 2011 Sixth International Conference, Vienna; Rost, M., & Bock, K. (2011). *Privacy by Design* and the New protection goals (pp. 9): Europrise, European Privacy Seal.

Privacy by Design Application Areas

1. CCTV/Surveillance Cameras in Mass Transit Systems;
2. Biometrics Used in Casinos and Gaming Facilities;
3. Smart Meters and the Smart Grid;
4. Mobile Devices & Communications;
5. Near Field Communications (NFC);
6. RFIDs and Sensor Technologies;
7. Redesigning IP Geolocation Data;
8. Remote Home Health Care;
9. Big Data and Data Analytics.

The Fundamentals

Privacy: A Practical Definition

From a practical perspective, privacy is not about secrecy or preventing organizations from collecting needed personal information as part of their role in providing goods or services to their customers. Privacy is about control – maintaining personal control over the collection, use, and disclosure of one's personally identifiable information. It is best expressed by the German concept of "informational self-determination," a term first used in the context of a constitutional ruling related to personal information collected during Germany's 1983 census.

In an age of complex, advanced networked systems and information communications technologies (ICTs), privacy challenges grow exponentially and often test the effectiveness of privacy legislation. There are those who would argue that the premise of individual control is unsuited to address the new class of privacy risks associated with social networking systems (SNSs). While context is critical to privacy, and existing views of privacy will need to evolve to address user-generated issues raised by SNSs as well as other Web 2.0 services, control will remain a cornerstone of privacy interests. The contextual approach to privacy should complement the empowerment of individuals to make their own choices regarding the dissemination of their personal data, rather than preclude the decision-making capacity of individuals on the basis of a "what if" or counterfactual analysis.

Today, "informational self-determination" remains a useful concept for practitioners tasked with implementing privacy practices in their organizations or designing privacy into information technologies and systems. The data subject or end-user must be at the heart of what drives the design and operational decisions concerning personal information.

When comparing the leading privacy practices and codes from around the world, there are principles and values that remain timeless and relevant to the age of the Internet. One noteworthy enhancement that needs to be recognized is the concept of data minimization. This reflects the view that programs, information technologies and systems should operate with non-identifiable interactions and transactions, as the default condition. Wherever possible, identifiability, observability and linkability of personal information should be minimized. In his book Code 2.0 (2006), U.S. academic Lawrence Lessig famously wrote, "Code is Law." He notes: "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." By extension, he demonstrated that we could, and should, engineer cyberspace to reflect and protect our fundamental values.

There are two essential Fair Information Practices (FIPs) that best characterize the essence of data privacy – "purpose specification" and "use limitation." Simply put, purpose specification speaks to clearly identifying why an organization needs to collect personal information. Use limitation refers to only using the data collected for the primary purpose specified. If the data collected will be used for other secondary purposes, then the individual must be informed and allowed to consent to the additional uses of his or her personal data.

These perspectives are fundamental to *Privacy by Design* (*PbD*) and inform its 7 Foundational Principles.

The 7 Foundational Principles of *Privacy by Design*

Privacy by Design – embedding privacy into information technologies, business practices, and networked infrastructures, as a core functionality, right from the outset – means building in privacy right up front – intentionally, with forethought. *PbD* may thus be defined as an engineering and strategic management approach that commits to selectively and sustainably minimize information systems' privacy risks through technical and governance controls. At the same time, however, the *Privacy by Design* approach provides a framework to address the ever-growing and systemic effects of ICTs and large-scale networked data systems with enhancements to traditional FIPs. These are: 1) acting proactively; 2) making privacy the default condition; 3) embedding privacy directly into design; and 4) taking a doubly-enabling positive-sum (not zero-sum) approach in the face of multiple, competing objectives.

What does it mean to practice these principles? Operationalization is essential to *PbD*. It extends the principles to a set of actionable guidelines that application and program owners can communicate to those responsible for their implementation. Think of the 7 Principles as a multi-pronged approach to achieving the highest standard of privacy protection, in an ecosystem requiring broad participation.

The approach will vary depending upon the organization, the technology and other variables. While there is no single way to implement, operationalize, or otherwise roll out a *PbD* -based system, taking a holistic approach is key. The process necessarily challenges programmers and engineers to think creatively about all of a system's requirements, and similarly challenges organizational leaders to innovate, test, and discover what works best in their particular environment.

What is certain is that when these principles are applied early on, robustly, systematically, and across the business ecosystem, they help to foster an environment where privacy harms are minimized or prevented from happening in the first place. They also stimulate:

- clear privacy goal-setting;
- systematic, verifiable methodologies;
- practical solutions and demonstrable results; and
- vision, creativity, and innovation.

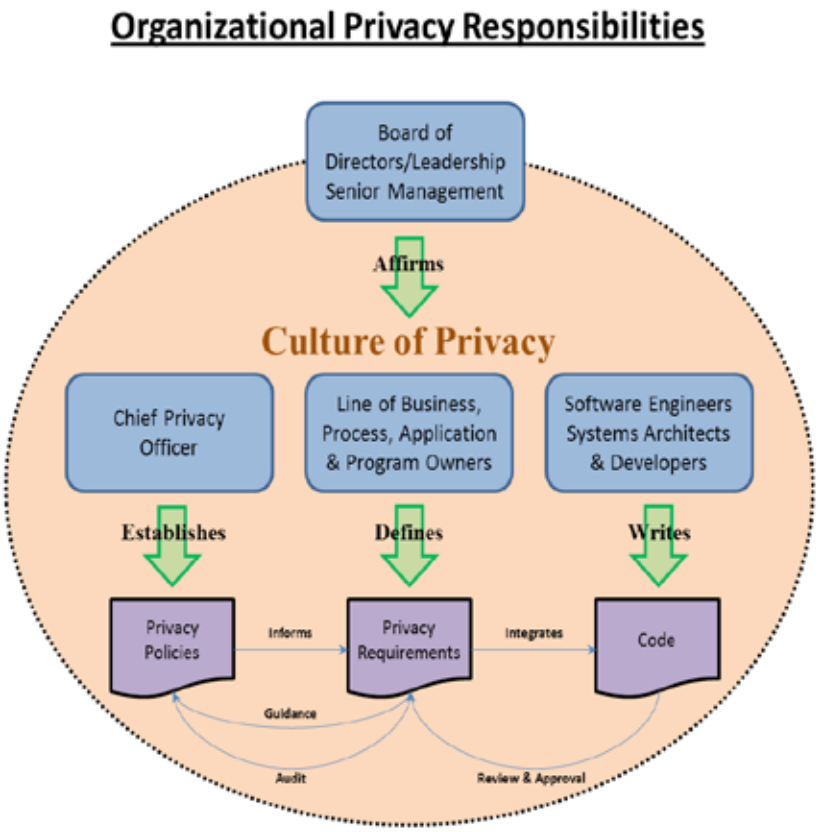
Examining the experiences of leading organizations in the application of the principles of *Privacy by Design* is profoundly instructive, suggesting paths forward for others interested in taking a comprehensive approach to responsible information management practices.

> *"The day started out with the Information and Privacy Commissioner of Ontario, Canada – Dr. Ann Cavoukian – giving a presentation via video to the group on Privacy by Design. … Now I have heard of Dr. Cavoukian and the* PbD *movement. But I had never been exposed to any details. The details were amazing and I like the 7 Foundational Principles. … These are sound principles that make a lot of sense."*
>
> **Craig Burton, KuppingerCole blog on The 2012 International OASIS Cloud Symposium, October 17, 2012**

Implementation Guidance

Organizations range from small (i.e. a sole proprietorship) and medium-sized to the very large (e.g. multinational corporations and governments) with structures that may be entrepreneurial, hierarchical, functional, divisional or matrix (to name a few). Regardless of their size and structure, however, any organization that encounters personal information must effectively manage and protect it.

Everyone within the organization has a role to play with respect to the protection of Personally Identifiable Information (PII). Yet this fails to bring us closer to appreciating precisely who is responsible for what. To begin that discussion, we propose the following model:



The integration of privacy and the development of customer or citizen-facing offerings is based on a set of privacy requirements, which, themselves, are reflected in an organization's privacy policies. The model recognizes that one or more individuals may perform some or all of the roles identified. What is important is not that an organization explicitly identifies an individual responsible for each role; rather, *that each of the tasks is undertaken and accountably executed.* For example, in a very small business, the founder may play the role of "Board/CEO" and "Chief Privacy Officer," while a colleague or subordinate may act as the "Application Owner" and "Programmer."

Privacy policies support a culture of privacy. Intended to apply across the organization, responsibility for their development and enforcement naturally falls to a senior member of the leadership team – ideally a CPO. A properly defined set of privacy policies forms a backdrop against which application owners and product developers develop specific sets of privacy requirements to be embedded into their offerings. A CPO's executional responsibility is associated with the development of practices to ensure that privacy is consistently embedded in applications and processes, and to audit them periodically to ensure that this is the case.

Privacy requirements are at the core of *PbD* execution. Informed by an organization's privacy policy, the 7 Foundational Principles of *PbD* and assisted by a variety of privacy-supportive processes and practices, those deemed to "own" the customer-facing offerings bear primary executional responsibility to ensure the development of a rich set of privacy requirements, as well as their subsequent integration in the development process – from the outset. Further, through the offering's development lifecycle, working with the developers, they must ensure that the requirements are satisfied and that deficiencies are identified and addressed. Once the development process is complete, its approval affirms that each of the requirements has been fully satisfied. Seeking guidance or assistance, should it be required, and updating the CPO regarding the completed offering's privacy status, rounds out the application owners' privacy responsibilities.

Based on their understanding of the offering's full suite of requirements, developers would then create the actual offering. They will most likely need to innovate to satisfy *PbD*'s central promise of "Full Functionality – Positive-Sum, not Zero-Sum." Over time, however, as privacy requirements become more commonplace, the task of embedding privacy will become simplified and accelerated by the development of "privacy code libraries" – collections of code that satisfy typical privacy requirements – similar in nature to those which currently exist for other purposes.

A variety of organizations have begun to undertake significant *PbD*-based implementations, and early indications suggest that a "one size fits all" approach may not be appropriate. To better understand this, we must build our experience and then assess the lessons learned. Working with several organizations and subject matter experts, my office has documented a range of *PbD* implementations in nine different areas (as noted earlier), reflecting a wide array of technologies.

The next section begins the process of systematizing and summarizing the lessons learned implementing the 7 Foundational Principles that have formed the cornerstone of our collection of *PbD* papers.

In this section, a consistent approach has been employed to assist those who seek to implement the principles of *PbD*. Each principle is identified and defined with key dimensions of the principle highlighted. A chart summarizes the "Actions" to implement the spirit of the principle that are most closely associated with the principle and who within the organization is accountable for their execution. Each principle is then informed by the insights gained by working with organizations that have implemented *PbD*-based privacy programs, as well as lessons learned from our long history of research in this area.

The 7 Foundational Principles of *Privacy by Design*

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 Setting***

We can all be certain of one thing – the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. 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 Security – ***Full Lifecycle Protection***

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

6. ***Visibility*** and ***Transparency*** – Keep it ***Open***

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

7. ***Respect*** for User Privacy – Keep it ***User-Centric***

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

Principle 1

Proactive not Reactive; *Preventative* not Remedial

Operational Guidance: *These actions anticipate and prevent privacy invasive events* ***before*** *they happen. Do not wait for privacy risks to materialize –* ***the aim is to prevent the breaches from occurring****.*

Actions	Responsibility
1. Affirm senior leadership commitment to a strong, proactive privacy program. 2. Ensure that concrete actions, not just policies, reflect a commitment to privacy. Monitor through a system of regularly reviewed metrics. 3. Develop systematic methods to assess privacy & security risks and to correct any negative impacts, well before they occur. 4. Encourage privacy practices demonstrably shared by diverse user communities and stakeholders, in a culture of continuous improvement.	Leadership/Senior Management e.g. Board of Directors, CEO, CPO, CIO, COO, CSO, Company Owner(s)

Organizations must begin with an explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently. Addressing privacy at the outset, prevents privacy issues from arising in the first place. This is the essence of *Privacy by Design* and a dimension where it exceeds traditional compliance frameworks. The alternative is privacy by chance, or worse, privacy by disaster (a term coined by Dr. Kai Rannenberg) – harried efforts to limit or remediate the damage that has already been done. In our view, that is too little, too late, and represents how things were done in the past.

> *Intel views* Privacy by Design *as a necessary component of our accountability mechanisms that we implement in our product and service development processes.*
>
> **David A. Hoffman, Director of Security Policy and Global Privacy Officer, Intel Corporation**

With *PbD*, clear commitments must be made and resources allocated to back them up. This kind of executive-led approach fosters the development of a culture of privacy across the entire organization. Such a culture enables sustained collective action by providing staff with a similarity of approach, outlook and priorities. It is what leads privacy to be woven into the fabric of the day-to-day operations of an organization, at all levels, and supports the ultimate success of an organization's privacy programs.

Accountability must be ensured, with clearly identified "business owners" who take on lead responsibility. In this sense, a "business owner" is understood to be an individual who has been explicitly identified as being accountable for the successful execution of one or more privacy-related tasks. These may be executives, organizational privacy leaders, business process owners, or project leaders. The Chief Privacy Officer, for example, is the "owner" of the organization's privacy policy. Similarly, a Brand or Product Manager is the "owner" of a product or service and is accountable for its management of the PII with which it comes in contact. The rise of the Chief Privacy Officer (CPO) role in organizations is a testament to the strategic importance of good information management.

Guidance for Boards of Directors: What You Don't Know *Can* Hurt You

Being proactive means that corporate directors, faced with a wide array of responsibilities arising from their board membership, must make oversight of the organization's privacy policies and procedures an integral and necessary component of effective board service. This can be achieved through the following actions:

a) Education is key – directors should ensure that they receive appropriate training in privacy and that there is someone with privacy expertise on their board;

b) Directors should ensure that at least one senior manager has been designated to be accountable for the organization's privacy compliance;

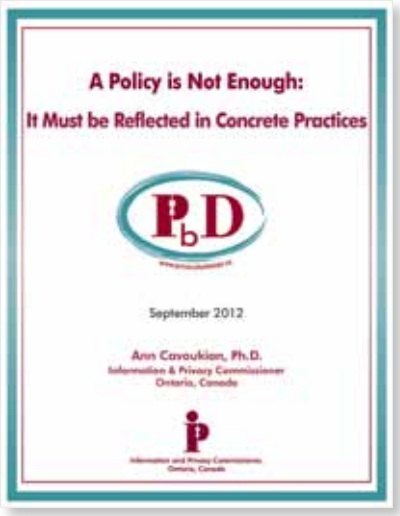
c) Directors should ensure that privacy compliance is a part of senior management performance evaluation and compensation;

d) Directors should ask senior managers to undertake periodic privacy self-assessments and privacy audits and to report to the board on these activities on a regular basis; and

e) Directors should ensure that they ask senior management the right questions about privacy practices in their organization.

Source: *Privacy and Boards of Directors: What You Don't Know Can Hurt You, November 2003* (*Revised July 2007*).

Guidance for Leadership: A Privacy Policy is Not Enough – It Must be Reflected in Concrete Practices



By itself, a privacy policy cannot protect the personal information held by an organization. To be proactive, the organization's privacy program must be reflected in actual practice or actions. This can be achieved by taking the following actions:

a) Implement a privacy policy that reflects the privacy needs and risks of the organization, and consider conducting an effective Privacy Impact Assessment;

b) Link each requirement within the policy to a concrete, actionable item – operational processes, controls and/or procedures, translating each policy item into a specific practice that must be executed;

c) Demonstrate how each practice item will actually be implemented;

d) Develop and conduct privacy education and awareness training programs to ensure that all employees understand the policies/practices required, as well as the obligations they impose;

e) Designate a central "go-to" person for privacy-related queries within the organization;

f) Verify both employee and organizational execution of privacy policies and operational processes and procedures; and

g) Proactively prepare for a potential privacy breach by establishing a data breach protocol to effectively manage it.

Source: *A Policy is Not Enough: It Must be Reflected in Concrete Practices, September 2012.*

Of course, the optimal time to be proactive is when an information technology or a networked infrastructure is new and emerging. By building privacy in from the outset – ideally as early as the conceptual stage, it becomes possible to foster confidence and trust in the technology or infrastructure as being privacy-protective, and ideally avoiding costly future retrofits.

Commonly referred to as a Privacy Impact Assessment, PIA methodologies vary in timing, application, breadth, transparency, and levels of prescription, among other dimensions. A significant milestone in the development and adoption of PIAs was the industry-led RFID (Radio Frequency Identification) PIA Framework approved by the EU in 2011 for demonstrating "Privacy by Design" compliance with the EU Data Protection Directive. In some circumstances, a PIA may be conducted alongside a security threat/risk assessment, which is one of the inputs into assessing the overall privacy landscape. Similarly, a PIA may also serve as a useful tool to be proactive about privacy during the early stages of conceptualization, when several options are under review.

All PIAs should have a modular nature, since most policies, governance frameworks and systems are neither the purview nor the expertise of a single person. For that reason, the PIA should have a coordinator or point person within the organization, often the Chief Privacy Officer. The CPO or other privacy lead should assemble the organizational team required to review and answer the PIA questions. In a corporate setting, that team would include representatives from IT, customer service, security, marketing, risk management, and relevant lines of business.

This approach serves to provide greater meaning for participants not directly responsible for privacy, and acts as a building block of the organization's information governance and risk management program. Optimally, the various owners/operators of the systems and other framework elements will have been consulted in the development of the PIA, and the PIA process will yield benefits to them, as well.

Conceiving of the PIA in this way helps those disciplines not specifically focused on privacy 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.

By conducting this type of assessment proactively and early on, the privacy impacts of the resulting technology, operation or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration or error during the implementation.

Guidance on Conducting a *Privacy by Design* Privacy Impact Assessment

Many existing PIAs focus primarily on an organization's compliance with legislative and regulatory requirements and FIPs. The *PbD*-PIA goes beyond regulatory compliance. The scope of this framework is broader and reflects *PbD's* holistic approach to privacy by transforming how an organization manages the privacy of individuals from policy and compliance to an organization-wide business issue and/or strategy that leads to being proactive rather than reactive.

a) The framework should be applied continuously at all stages (conceptual, physical and logical) of the design, development and implementation of the information technology, business process, physical space and networked infrastructure project;

b) Organizations should take into consideration the privacy expectations of individuals regarding their information;

c) Privacy and data protection practices and controls need to be present and continually assessed, including a comprehensive assessment of the governance of, and accountability for, PII by considering an organization's privacy and data protection practices in their entirety; and

d) Appropriately assesses privacy and security in tandem throughout the analysis process.

Source: *Pat Jeselon and Anita Fineberg (co-authors) – A Foundational Framework for a PbD - PIA, November, 2011.*

Just as no single designer can achieve privacy within an organization, no single organization can achieve privacy within an industry. "*Privacy by Design* is a team sport." Privacy must be considered in an ecosystem-wide manner if it is to be both effective and lasting in broad networked sectors such as the mobile communications industry.

Guidance on Proactively Applying Privacy in a Federated Ecosystem

The New Federated Privacy Impact Assessment or (*F-PIA*) is a practical assessment of how privacy can be proactively applied to a group of organizations and businesses that wish to create a community to manage their clients' identity – one that is based on trust. It is based on a realization that privacy protection is not available in a standard one-size-fits-all model. Each business is unique, and privacy needs are equally unique. The *F-PIA* differs from a traditional PIA in a number of ways. Most importantly, the *F-PIA* is designed to operate, either within an enterprise (such as one where a number of different systems may be federated together) or across enterprises that have different needs and uses of personal information. It should:

a) Provide an opportunity for members to discuss, develop and codify a Federation's privacy policies;

b) Demonstrate that privacy policies, as defined by the members of the Federation, will be met;

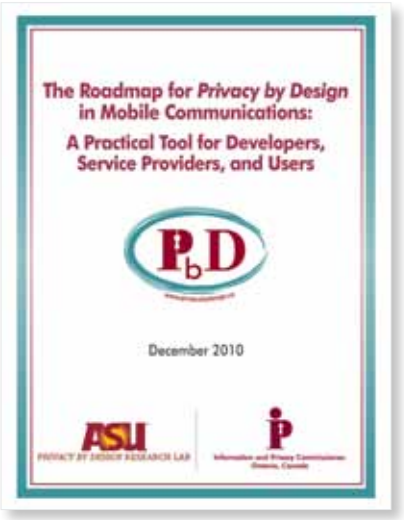
c) Demonstrate that an appropriate technological architecture is in place to prevent, to the greatest extent possible, accidental or malicious violations of privacy policies; and

d) Benefit all parties who complete, use and rely on an *F-PIA*.

Source: *Joseph H. Alhadeff (co-author on behalf of the Liberty Alliance Project) – The New Federated Privacy Impact Assessment (F-PIA) Building Privacy and Trust-enabled Federation, January 2009.*

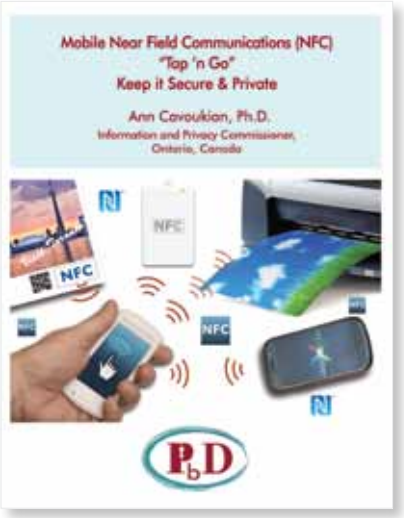
Guidance on Proactively Applying Privacy in the Mobile Ecosystem

To be truly proactive, the hallmark for success of a *PbD* initiative, collaborative efforts across various stakeholders must be undertaken. This is particularly well illustrated by the *Mobile Communications Industry Roadmap* developed in cooperation with an expert industry panel convened for the Arizona State University (ASU) *Privacy by Design* Research Lab's study on mobile technologies. This Roadmap identifies key responsibilities for each player individually, but also reflects the need to take a collective approach among the players of an industry ecosystem including the Device Manufacturers, OS/Platform Developers, Network Providers, through to the Application Developers and the Consumer. The detailed design recommendations are outlined under Principle 3: "Privacy ***Embedded*** in Design."



Source: *Marilyn Prosch (co-author, ASU Privacy by Design Research Lab) – The Roadmap for* Privacy by Design *in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users, December 2010.*

Guidance on Proactively Applying Privacy into Disruptive Wireless Technologies and Standards

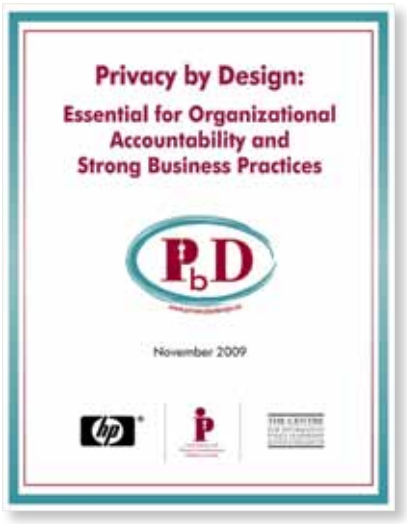


Near Field Communications (NFC) or "Tap 'n Go" (conveying a visual image in which this technology is intended to be used) is an ecosystem that includes the NFC Forum, NFC Device Manufacturers, NFC Application Developers and Businesses developing NFC service use cases (such as smart posters, mobile operators and individual users). In addition, the NFC ecosystem interacts with existing Internet and Web ecosystems and so should coordinate its security and privacy strategy with these other ecosystem stakeholders.

Source: *Nokia (co-author) – Mobile Near Field Communications (NFC) "Tap 'n Go" - Keep it Secure and Private, November 2011.*

Guidance on Practices that Support a Culture of Continuous Improvement in Privacy Protection: Organizational Tools and Frameworks

The following papers provide examples of approaches to organizational tools and frameworks that have been developed to support proactive privacy practices:



a) The development and deployment of Hewlett Packard's Accountability Model Tool for employees provides an interesting case study of how privacy practices can support a culture of continuous improvement.

Source: *Co-authored with Martin E. Abrams (Centre for Information Policy Leadership, Hunton & Williams LLP), Scott Taylor (Hewlett-Packard) – Privacy by Design: Essential for Organizational Accountability and Strong Business Practices, November 2009.*

b) IBM was an early adopter of *PbD* and demonstrated how the *PbD* principles guide the architectural foundation of an enterprise's global operations. This strategic and proactive focus on privacy has enabled process improvements that demonstrably link to reduced operational costs and that support IBM's business strategy. IBM took a three-pronged approach to reinforce its strong privacy policies by implementing privacy practices within its large, diverse and global organization using online tools. To ensure that its privacy practices were adopted broadly across the enterprise, three online tools have been deployed enterprise-wide: i) a Privacy Self-Assessment tool; ii) a tool for Privacy Education and Awareness Training; and iii) a Web-based Data Incident Management tool. Having been successfully implemented at IBM, these *PbD* tools have demonstrated how organizations of any size can be proactive about privacy.

Source: *Co-authored with Yim Chan, IBM* – Privacy by Design*: From Policy to Practice, September 2011.*

c) The YMCA and Ontario Lottery and Gaming Corporation (OLG) introduce privacy risk management practices that organizations can establish as an organizational framework for being proactive about risks to personal information.

Source: *Co-authored with YMCA, OLG – Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default, April 2010.*

d) Nymity's *PbD* Risk and Control Checklists support its Privacy Risk Optimization Process (PROP) that is based on the International Organization for Standardization (ISO) concept that risk can be both positive and negative. Risk Optimization is a process whereby organizations strive to maximize positive risks and mitigate negative ones. The PROP uses these concepts to implement privacy proactively into operational policies and procedures.

Source: *Co-authored with Terry McQuay (Nymity Inc.)– A Pragmatic Approach to Privacy Risk Optimization:* Privacy by Design *for Business, August 2009.*

> *I want to congratulate you on the incredible achievement of what I would call the* Privacy by Design *movement. Based on the OECD and International Data Protection and Privacy Commissioners' conferences in Israel it is clear that industry, government and NGOs have all embraced* PbD *everywhere in the world. I say this based on both the conversations I had with individuals and the sessions I attended. People understand and seem committed.*
>
> **Terry McQuay, President, Nymity Inc.**

e) Ontario's Independent Electricity Service Operator (IESO) developed internal control systems to protect smart meter data. The controls are based on essential preconditions, including support for building in privacy, across the full range of IESO's Board of Directors, management and other stakeholders. In addition, a process was established to manage risks effectively, while making information available to the public and key stakeholders on the IESO's and the Smart Metering Entity (SME) website, such as governance documents, manuals, procedures and key contact information. Also, the IESO proactively monitors and audits its controls that help support the objective of protecting smart meter data, by default.

Source: *Co-authored with IESO – Building Privacy into Ontario's Smart Meter Data Management System: A Control Framework, May 2012.*

Principle 2

Privacy as the *Default Setting*

Operational Guidance: *These methods seek to provide privacy assurance – delivering the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice.* ***No action should be required on the part of the individual user to protect their privacy*** *– it should be built into the system, automatically – by default.*

Actions	Responsibility
1. Adopt as narrow and specific a purpose(s) for data collection as possible – begin with no collection of personally identifiable information – data minimization.	Software Engineers & Developers
2. Minimize the collection of data at the outset to only what is strictly necessary.	Application & Program Owners
3. Limit the use of personal information to the specific purposes for which it was collected.	
4. Create technological, policy and procedural barriers to data linkages with personally identifiable information.	Line of Business & Process Owners

The single most effective yet most challenging method of preserving privacy is to ensure that the default settings – the settings that apply when the user is not required to take any action – are as privacy-protective as possible. In operationalizing this principle, one might think of the discipline of engineering privacy being examined by a number of academics (e.g. S. Gurses, C. Troncosco and C. Diaz; 2011) on which there will be reliance when dealing with back-end systems. Privacy management as a distinct discipline is becoming more standardized and professionalized, with a growing demand for skilled privacy engineers and architects. We want to encourage thinking beyond the default settings associated with preferences that users can manually control, and to consider the overall system defaults.

The starting point for designing information technologies and systems must always be maximally privacy-enhancing, beginning with NO collection of personally identifying information, unless and until a specific and compelling purpose is defined. If this is the case, organizations should seek to adopt as narrow and specific a purpose(s) for data collection as possible. "Specified purposes should be clear, limited and relevant to the circumstances."

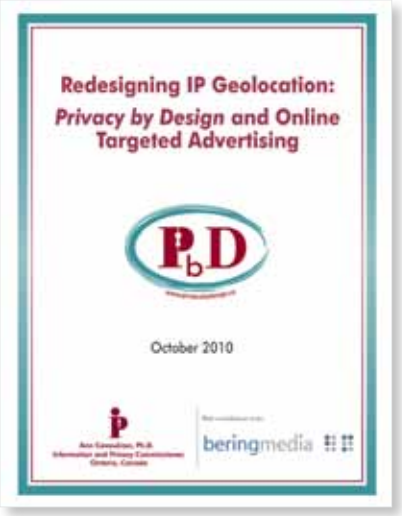
This approach, referred to as "data minimization," must be the first line of defence – non-collection, non-retention and non-use of personal data. Similarly, the collection, use and disclosure of aggregated or de-identified personal information raise few, if any, privacy issues. Quite simply, personal data that is not collected, retained, or disclosed needs no securing, management, or accounting – no duty of care arises, nor possibility of harm. Likewise, personal data that does not exist in a database cannot be accessed, altered, copied, appended, shared, lost, hacked, or otherwise used for secondary purposes by unauthorized third parties. All too often, we apply the same requirements from the paper world to the digital world when in fact, online systems require less data precisely because of the mathematical and computational capabilities of technologies.

Where personal data must be collected for clearly specified purposes, the next step in operationalizing this principle is to limit the uses and retention of that information, as much as possible. The principles of purpose specification and use limitation, contained in FIPs, best illustrate this point.

There are many ways in which this may be accomplished. One method is to carry out operations with privacy implications (i.e. those that use personal information) client-side – that is, entirely under the control of users and their devices. Obviously, the more tamper-proof, secure, and user-controlled the device or software, the more trusted it will be to carry out its functions reliably. Dividing data, functions, and roles among different entities is a proven method of ensuring privacy. For example, this strategy is the basis for using proxy servers to obscure IP addresses and to defeat online tracking and profiling. In practice, a combination of organizational and technical measures will be necessary to achieve this goal of default privacy.

The default principle is illustrated in the following examples:

1. **Location Based Services:** Ad Serving by Geolocation – The technology developed by Bering Media, Inc. allows Internet Service Providers (ISPs) that have made the decision to partner with an ad server to provide geolocation services with zero disclosure of potentially personally identifiable information about subscribers. Their "double-blind" privacy architecture allows the ISP to collaborate with an ad server without the need for reading or modifying any packets travelling through the network. Two additional privacy technologies – minimum match threshold and anti-inference algorithms – were developed and integrated into the double-blind privacy architecture to ensure, by default, that all campaigns always meet sufficiently large aggregate privacy counts to properly address re-identification risks.



Source: *Michael Ho, Co-author, Bering Media – Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising, October 2010.*

2. **Face Detection Not Face Recognition:** Embedding Privacy into Anonymous Digital Signage – This system is designed, by default, to avoid collecting, transmitting or retaining any identity information about viewers. Innovative digital signage technology, developed by Cognitech in Ontario, detects the presence of viewers, estimates their age and gender, and serves them customized content, all anonymously. The technology uses pattern detection algorithms to scan real time video feeds, looking for patterns that match the software's understanding of faces. The data is logged and the video destroyed on the fly – with nothing in the process recognizing the individuals who passed by in front of the sensors.

Source: *With support from Intel – White Paper: Anonymous Video Analytics (AVA) technology and privacy, April 2011.*

3. **De-Identification of Health Data:** De-identified data is information that has had its identifiers removed, but has not been combined or aggregated with other individuals' data. It is a common approach to privacy protection and as a general rule can help protect personal information in the event it is lost or stolen, making it more difficult to exploit for nefarious purposes. Re-identification is extremely difficult in practice when appropriate de-identification techniques are used. While de-identification remains an important tool, the first approach should be data minimization in which data aggregation ensures that individual data is not disclosed in the first place. Advanced de-identification methods

allow data custodians to exploit data without risking identity. Dr. Khaled El Emam, Canada Research Chair in Electronic Health Information, CHEO Research Institute and University of Ottawa, has developed methodologies and de-identification algorithms to manage risks related to re-identification, data theft and misuse.

Sources: *Khaled El Emam, Ph.D., Co-author (Canada Research Chair in Electronic Health Information, CHEO Research Institute and University of Ottawa) – Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy, June 2011; A Positive-Sum Paradigm in Action in the Health Sector, March 2010.*

4. **Privacy-Enhanced Biometric Identifiers:** Biometric Encryption – This cryptographic algorithm ensures that biometric data are not connected to any personal data, by default. Further, the biometric data is prevented from being used by another system that is capable of connecting biometric data to any personal information. Biometric Encryption securely binds a PIN or a cryptographic key to a biometric and the key may only be recreated if the correct live biometric sample is presented upon verification. The digital key (password, PIN, etc.) is randomly generated on enrolment, so that even the user (or anyone else) does not know it. The key itself is completely independent of the biometric and, therefore, can always be changed or updated. After a biometric sample is acquired, the BE algorithm securely and consistently binds the key to create a protected BE private template. In essence, *the key is encrypted through the biometric.* BE provides excellent privacy protection and can be stored either in a database or locally (smart card, token, laptop, cellphone, etc.). At the end of the enrolment process, both the key and the biometric are discarded.

Source: *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy, March 2007.*


Adding an On/Off Device to Activate the RFID in Enhanced Driver's Licences:
Pioneering a Made-in-Ontario Transformative Technology that Delivers Both Privacy and Security

5. **RFID On-Off Transmission Control:** With a vicinity read RFID chip embedded inside, the Enhanced Driver License (EDL) was intended to communicate with readers at U.S. customs and border crossings in order to enhance identity checks. This RFID remained "on" by default, posing significant privacy risks to the bearers. A *Privacy by Design* approach argued that the default transmission setting for these cards should be "off" until users chose to turn it on.

Source: *Adding an On/Off Device to Activate the RFID in Enhanced Driver's Licences: Pioneering a Made-in-Ontario Transformative Technology that Delivers Both Privacy and Security, March 2009.*

User Deactivation Not Destruction: A privacy-protecting RFID tag, known as the "clipped tag" was developed by IBM for the retail sector. The clipped tag put the option of privacy protection in the hands of the consumer and addressed the reactivation issue. After the sale, a consumer may tear off a portion of the tag, much like the way in which a ketchup packet is opened. This transformed the long-range tag into a proximity tag that could still be read, but only at short range – less than a few inches or centimeters. The modification of the tag may be confirmed visually. The tag may still be used at a later time for returns, recalls, or experiencing a product warranty.

Sources: *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum, March 2009; Video: A Word About RFIDs and your Privacy in the Retail Sector, March 2006.*

6. **Distributed Information Privacy Architecture:** Separating Domains in Service-Oriented Architecture in the Smart Grid. Ontario's Hydro One utility used the concept of "Domains" to classify the possible implications for privacy in the Smart Grid and to impose certain architectural decisions to meet privacy requirements. The three domains identified were: Customer Domain, Service Domain, and Grid Domain. As a result of the analysis, the default designed into the energy utility's Advanced Distribution System (ADS) separated the various data domains and conducted data aggregation on consumer data in a dynamic manner.

Source: *Hydro One, GE, IBM, Telvent (Co-authors) – Operationalizing Privacy by Design: The Ontario Smart Grid Case Study, February 2011.*

Principle 3

Privacy *Embedded* into Design

Operational Guidance: *These actions embed privacy requirements into the design and architecture of IT systems and business practices. They are* ***not bolted on as add-ons, after the fact****. Privacy should be an essential component of the core functionality being delivered.*

Actions	Responsibility
1. Make a Privacy Risk Assessment an integral part of the design stage of any initiative, e.g. when designing the technical architecture of a system, pay particular attention to potential unintended uses of the personal information.	Application & Program Owners
2. Base identity metasystems on the "Laws of Identity," intended to codify a set of fundamental principles to which universally adopted, sustainable identity architecture must conform.	Line of Business & Process Owners
3. Consider privacy in system development lifecycles and organizational engineering processes. System designers should be encouraged to practice responsible innovation in the field of advanced analytics.	Software Engineers & Developers
4. Embed privacy into regulatory approaches that may take the form of self-regulation, sectoral privacy laws, omnibus privacy legislation and more general legislative frameworks, calling for an approach guided by "flexibility, common sense and pragmatism."	Regulators

Operationalizing this Principle requires approaching design and development processes throughout the organization in holistic, integrative and creative ways. Just as *PbD* represents a shift in the way that organizations think about privacy – moving away from a reactive model to a proactive one – enshrining *PbD* in regulatory instruments, voluntary codes and best practices requires a shift in how law and policy-makers approach rule making. What is invited is the development of innovative approaches to promoting and enshrining privacy in various instruments.

What is essential is that all interests and objectives, including privacy, be clearly documented, desired functions articulated, metrics agreed upon and applied, and trade-offs rejected as being unnecessary, in favour of finding a solution that enables multi-functionality (see Principle 4: Full Functionality – ***Positive Sum***, not Zero-Sum).

At the same time, information security system standards and frameworks are being applied today by enterprises, in greater numbers and with greater rigour, and Enterprise Architecture design has burgeoned as a discipline, fuelled in part by regulatory and competitive pressures. These information management efforts are consistent with, and can inform, Principle 3: Privacy ***Embedded*** into Design.

Most important, even in scenarios where the target is an IT system or application, operationalizing *PbD* cannot be viewed exclusively as just an IT project. Privacy expertise must be available and engaged through all phases of the workflow, and bring with it a multi-faceted understanding of privacy issues and requirements, and an appreciation of consumer/client expectations. Depending on the nature of the project, there may be significant need for the competencies of functional experts, risk managers, process experts, and other specialists.

I called 2011 the "Year of the Engineer." In an effort to reach out to a wider spectrum of expert participants, I gave talks almost exclusively to software engineers in 2011, in an effort to engage a wide spectrum of software engineers, computer scientists, and technology developers from around the globe. Together, we started a dialogue about translating the 7 Foundational Principles of *PbD* into project requirements, procurements specifications, and positive-sum operational results. I was truly heartened by the warm response I received from the engineers I met with!

> *"Privacy by Design is a concept promoted by Ann Cavoukian, Ph.D., Information & Privacy Commissioner Ontario, Canada which aims to promote the idea of systems and processes built with privacy in mind, rather than retrofitted afterwards. I encourage all readers to browse her site which is quite informative, and gives you perhaps a "bigger picture" view than IT alone."*
>
> **Simon Hunt, Vice-President & Chief Technology Officer, McAfee Data Protection.**

Here are some illustrative examples of this work and the contributions to embedding *PbD* into engineering design:

1. **Anticipating Unintended Consequences of Networked Systems:** Embedding privacy into Wi-Fi protocols – We must research and think creatively to find ways to embed privacy into Wi-Fi protocols that can randomize MAC addresses or ensure privacy through a proxy-like method of assigning addresses. Innovative solutions will be required to change the existing model of using persistent MAC addresses that remain uniquely bound to a mobile device. For example, research in the area of IPv6 is attempting to ensure the privacy of IP address through a proxy-like method of assigning addresses.

Source: *Kim Cameron, Co-author (Identity Architect) – Wi-Fi Positioning Systems: Beware of Unintended Consequences, June 2011.*

2. **Embedding Privacy into Big Data Methods:** A responsible "Big Data analytic sensemaking" engine – Big Data is here and organizations want to leverage data analytics to maximize this growing resource. While organizations have practical incentives to make the most out of Big Data, we need to ensure that privacy is embedded into these systems. Jeff Jonas shows us how embedding *PbD* is possible with his sensemaking systems technology. We believe this design will guide others in the process of creating their own next-generation analytics. This not only demonstrates that privacy can be embedded into data analytics technologies but it can be done in a positive-sum manner. The sensemaking technology has been designed to make sense of new observations as they happen, fast enough to take action on them while the transaction is still happening. Since its analytic methods, its capacity for Big Data and its speed are game-changing, from a privacy perspective, it has been designed from the ground up with privacy protections in mind: i) full attribution, knowing the source of the data as well as data tethering (any revisions of the data) are turned on by default; ii) the analytics can be done on anonymized data or what we call data minimization; iii) there is a tamper-resistant audit logging feature that applies even to the database administrator which enhances transparency and accountability; iv) the false negative favouring methods reduce the number of incorrect identifications that may have a significant impact on civil liberties; v) self-correcting false positives advance greater accuracy in identification; and vi) the inclusion of information transfer accounting helps track secondary uses of the data. The dynamic pace of technological innovation requires us to embed privacy into design in a proactive manner – systems designers should be encouraged to practice responsible innovation in the field of advanced analytics.

Source: *Jeff Jonas, Co-author, (IBM)* – Privacy by Design *in the Age of Big Data, June 2012.*

3. **Embedding Privacy into Remote Surveillance Systems:** Ethical Technology in the Homes of Seniors (ETHOS) – A project with *Privacy by Design* – minimize data; make control meaningful; make control usable; and empower – don't overwhelm. This National Science Foundation-funded, Indiana University-Bloomington interdisciplinary team created a digital toolkit that enabled elders to maintain their privacy, while taking full advantage of home-based computing for their health and personal safety. Elders systematically underestimate their electronic privacy risk. This project examined the role of information technology in the homes of elders with an emphasis on design and evaluation for privacy. The ETHOS team is creating tools that will help elders make appropriate decisions about home-based computing and guide designers in creating privacy-respecting technologies.

Source: *L. Jean Camp, Ph.D. – Respect by Design. Paper presented at "*Privacy by Design*: The Gold Standard," Toronto, Ontario, January 2010.*

4. **Embedding Privacy into Mobile Location-Based Services:** Mobile applications and location-based services. This presentation provides an overview of solution approaches with privacy embedded into design such as PRIME/T-Mobile: LBS Application Prototype & Privacy Gateway, ISO/IEC JTC 1/SC 27/ WG 5 Identity Management considering Privacy and PICOS: Privacy for mobile social networks. Privacy and Identity Management for Europe (PRIME) aims to develop a working prototype of a privacy-enhancing identity management system for mobile platforms. The Privacy Gateway infrastructure component has been deployed at T-Mobile Germany and Deutsche Telekom and allows subscribers to set which application provider gets access to their data and when (date/time). PICOS is a demonstration of how privacy is designed into a mobile location application that allows for different partial identities for different usage contexts including limited disclosure of personal information for each partial identity.

Source: *Kai Rannenberg, Ph.D. –* Privacy by Design *in Mobile Applications and Location Based Services. Paper presented at "Privacy by Design: The Gold Standard," Toronto, Ontario, January 2010.*

5. **Embedding Privacy into Population Health Data:** Population Data BC (PopData) is an innovative leader in facilitating access to linked data for population health research. Researchers from academic institutions across Canada work with PopData to submit data access requests for projects involving linked administrative data, with or without their own researcher-collected data. PopData and its predecessor – the British Columbia Linked Health Database – have facilitated over 350 research projects analyzing a broad spectrum of population health issues. PopData embeds privacy in every aspect of its operations. This case study focuses on how implementing the *Privacy by Design* model protects

privacy while supporting access to individual-level data for research in the public interest. It explores challenges presented by legislation, stewardship, and public perception and demonstrates how PopData achieves both operational efficiencies and due diligence.

Source: *Caitlin Pencarrick Hertzman, Nancy Meagher, Kimberlyn M McGrail* – Privacy by Design *at Population Data BC: a case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest, August 2012.*

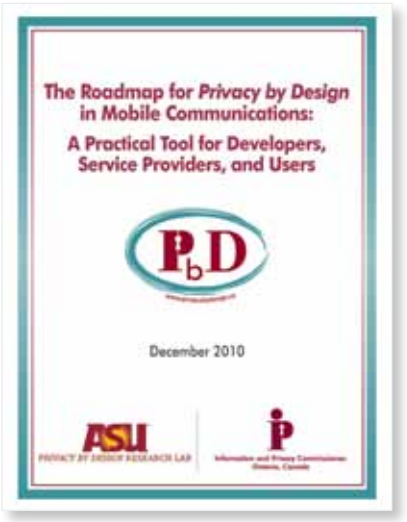
6. **Embedding Privacy into Smart Meter Devices:** Aggregation protocols and cryptographic techniques for smart meter implementation – Privacy is important to consider at the earliest stage when designing advanced metering systems. A lot of work has been done on a set of efficient privacy-preserving, built-in smart meter protocols that can fulfill a number of use case scenarios such as billing, network management and fraud control. Utilizing homomorphic encryption commitment schemes, computations can be done on the commitments without revealing the secrets. These techniques provide utilities with the granular meter data needed for load management, billing, and fraud or other security functions, without necessarily revealing detailed individual meter readings. They have been implemented and tested both as a PC implementation and on smart meter production models (Elster SG) with positive results and show no impact on functionality.

Source: *Ann Cavoukian & Klaus Kursawe – Implementing* Privacy by Design*: The Smart Meter Case. Paper presented at "the IEEE International Conference on Smart Grid Engineering (SGE'12)," Oshawa, Ontario* (*to be published).*

7. **Embedding Privacy into Utility Networks and Systems:** A case study by an electrical utility – This report chronicles San Diego Gas & Electric's (SDG&E) early stage incorporation of privacy into its Smart Pricing Program design cycle. The project team considered how to ensure user privacy right from the beginning of the project by clearly spelling out the privacy requirements and making them a high priority. The mechanisms identified to make privacy an essential design feature were an Enterprise Architecture Privacy Viewpoint, Enterprise Architecture Privacy Principles, Privacy Quality Assurance Checklist and Draft of Privacy Controls in Security Requirements. Privacy is a required feature in all requests for proposals to develop technologies associated with the project.

Source: *Caroline Winn, Co-author, (San Diego Gas & Electric) – Applying* Privacy by Design *Best Practices to SDG&E's Smart Pricing Program, March 2012.*

8. **Embedding Privacy into Mobile Technologies and Ecosystems:** These are examples of privacy design features specific to the mobile industry:



a) Mobile Device Manufacturer:

- Build in any protections that can be made independent of the OS/Platform/Application (e.g. automatic encryption of stored data);
- Build in privacy/security tools required by other developer levels (e.g. multi-factor authentication);
- Build in simple data wipe mechanisms for end-of-life or phone loss/theft scenarios;
- Determine a means of digitally marking or separating roles (e.g. youth vs. adult, home vs. work); and
- Ship phones with potentially privacy-invasive features (e.g. geolocation information accessible by applications) turned **off**. If, for regulatory (e.g. emergency services must have access to geolocation information) or technical reasons, the geolocation capability or other functionality of the device cannot be turned entirely off, the default condition should be that such information is inaccessible to applications not covered by the regulation. This difference should be made clear to the user, however.

b) OS / Platform Developer:

- Design reporting features that allow the user to be notified of how data is being collected, by what applications, and whether any exceptions to his/her privacy preferences have occurred;
- Provide a simple, easy to understand user interface for such controls;
- Minimize applications' access to device data; and
- Where practical, define privacy requirements and security standards for services provided on the platform.

c) Network Providers:

- Educate users about the risks associated with personal information;
- Complete a threat risk assessment and conduct annual, independent third party privacy audits; and
- Work to create a federated identity management subsystem.

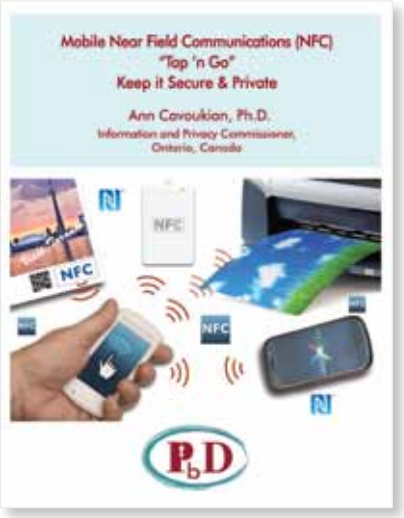
d) Application Developers / Data Processors:

- Integrate privacy into the development cycle, and practice data minimization techniques;
- Use privacy-protective default settings;
- Ensure end-to-end protection of user data;

- Maintain user awareness, and control of, data collection and use; and
- Design applications with privacy in mind.

Source: *Marilyn Prosch, Co-author, (ASU Privacy by Design Research Lab) – The Roadmap for* Privacy by Design *in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users, December 2010.*

9. **Embedding Privacy into Wireless Communications Ecosystems:** These are examples of the design requirements set out for NFC technology deployment.



   a) NFC Device Manufacturer: Consider the holistic, platform-wide solution being provided and the privacy design aspects that each component element in their design adds to the overall solution, to avoid the false assumption that privacy will be handled by some other component within their solution (e.g., NFC data transfer application assuming Bluetooth stack on the mobile device will inform the user of details of the data to be received).

   b) NFC Application Developer: When creating applications, especially within the peer-to-peer category, NFC application developers should also be cautious about design elements that create a persistent linkage of the NFC usage to the user or individual mobile device (e.g., MSISDN, IMEI, gamer player identifier "XYZ," etc.). The collection of personal information such as a unique device identifier should be featured in the notification provided to users.

Source*: Co-authored with Nokia – Mobile Near Field Communications (NFC) "Tap 'n Go" – Keep it Secure & Private, November 2011.*

10. **Embedding Privacy into Governance and Oversight Mechanisms:** Embedding *PbD* Principles into Regulatory Frameworks. This illustrates how addressing privacy proactively may be embedded into the design of regulatory frameworks. *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." Under the influence of such a "second generation" approach, incorporating the Principles of *Privacy by Design*, companies can be encouraged to go beyond mere regulatory compliance with notice, choice, access, security and enforcement requirements. 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.

Source: *With Foreword by Pamela Jones Harbour* – Privacy by Design *in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers, August 2011.*

Principle 4

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

Operational Guidance: *These actions seek to accommodate legitimate interests and objectives in a positive-sum, 'win-win' manner, not through a zero-sum (win/lose) approach, where unnecessary trade-offs to privacy are made. Avoid the pretense of false dichotomies, such as privacy vs. security – demonstrate that it is possible to have both.*

Actions	Responsibility
1. Acknowledge that multiple, legitimate business interests must coexist. 2. Understand, engage and partner – Practice the 3Cs – communication, consultation and collaboration, to better understand multiple and, at times, divergent interests. 3. Pursue innovative solutions and options to achieve multiple functionalities.	Leaders/Senior Management Application & Program Owners Line of Business & Process Owners Software Engineers & Developers

This principle rejects the widespread but erroneous view that privacy must always compete with other legitimate interests, design objectives, and technical capabilities, in a given domain. In the zero-sum view, in order to enjoy privacy, we must give up other functionalities that we value, such as security/public safety, system efficiency, flow of health-care information, or business interests – to name a few.

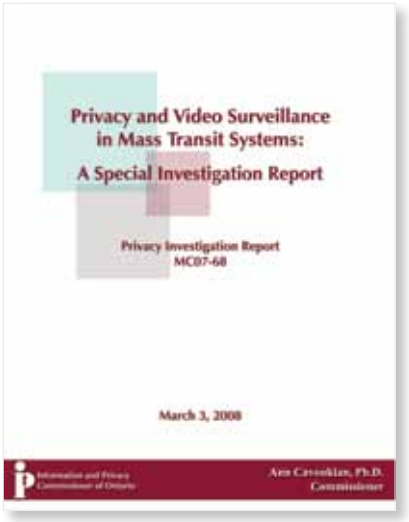
Perhaps nowhere has this outdated, yet mainstream, way of thinking been more apparent than in the area of public safety/security. This is where we see the classic zero-sum paradigm writ large, with the view that the more we have of one interest (public security), the less we can have of another (individual privacy). In this zero-sum framework, privacy can never win out – the other interest advances, always at the expense of privacy.

Similarly, in health care, tensions exist between the need to have vital health-care information readily available for treatment and care by health-care professionals yet at the same time, carefully guarded as highly sensitive data. Respecting people's privacy should never present an impediment to the delivery of health-care services. Given the sensitive nature of health-related information, these highly beneficial systems will only succeed if they are built with privacy in mind – thereby delivering a positive-sum, doubly-enabling outcome.

Although each of the IPC's repertoire of papers on *Privacy by Design* demonstrates the positive-sum principle, for the purposes of illustration, a selected few are used to illustrate how this principle is operationalized. By adopting a positive-sum paradigm and applying a privacy-enhancing technology to a surveillance technology, you develop what I call "transformative technologies." Among other things, transformative technologies can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive, serving to minimize the unnecessary collection, use and disclosure of personal data, and promoting public confidence and trust in data governance structures.

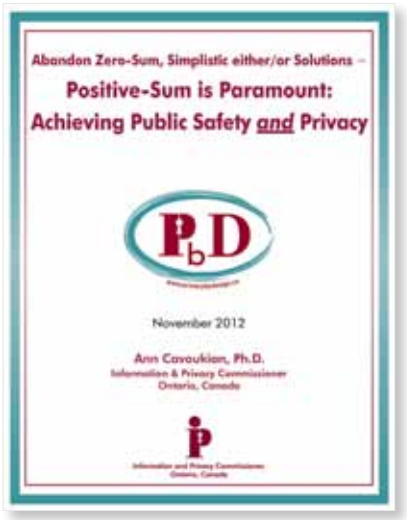
1. **Identifying Problem Gamblers *not* Loyal Patrons:** Identifying self-excluded gamblers ***and*** protecting the privacy of casino patrons – how do you achieve both objectives? Privacy-protective facial recognition allows for the use of video surveillance and facial recognition systems for the purpose of a watch-list scenario that helps to detect, identify and flag problem gamblers who have opted-into a problem gamblers/self-exclusion program. More importantly, the system was designed NOT to collect the biometrics of the millions of regular patrons who visit Ontario's casinos, racetracks and slot machines annually. By separating the facial recognition functions from the identification processes directly in the hardware, network and software, through the used Biometric Encryption, Ontario's Lottery and Gaming Corporation (OLG) is able to assure the privacy of millions of non-enrolled gamblers, whose biometrics are never collected, while providing maximum privacy to those in the self-exclusion program.

Source: *Tom Marinelli, Co-author, (OLG) – Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept, November 2010.*



2. **Protecting Public Spaces *and* Personal Privacy:** Video Surveillance Cameras in Public Spaces such as a Mass Transit system ***and*** privacy – There are a broad range of views about video surveillance and its impact on privacy. In the IPC's guidelines for the *Use of Video Surveillance Cameras in Public Places*, an effort was made to build in a positive-sum approach. When applied to the use of video surveillance by law enforcement, our experience has been an excellent example of this principle in action. Toronto Police Service Chief William Blair has pointed to *Privacy by Design* as a "positive-sum approach to the use of public space cameras in Toronto, one that enables the use of this additional tool to support policing, while concurrently mitigating privacy concerns through technological and operational design."

Source: *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report – Privacy Investigation Report MC07-68, March 2008.*



3. **Achieving Public Safety *and* Privacy:** This paper documents the positive-sum approach of *Privacy by Design* through collaboration, consultation and communication. It chronicles examples of successful initiatives and also initiatives that reflect a Privacy by Disaster approach.

Source: *Abandon Zero-Sum, Simplistic either/or Solutions – Positive-Sum is Paramount: Achieving Public Safety and Privacy, November 2012.*

4. **Health Data Research Without Compromising Patient Privacy:** Protecting sensitive health data ***and*** making it available for health research – Dr. Khaled El Emam, a senior investigator at the Children's Hospital of Eastern Ontario Research Institute (CHEO), and Canada Research Chair in Electronic Health Information, has resolved this issue through the development of a tool that de-identifies personal health information in a manner that simultaneously minimizes both the risk of re-identification and the degree of distortion to the original database. The application of this tool to any database of personal health information provides the highest degree of privacy protection, while ensuring a level of data quality that is appropriate for the secondary use. This privacy-enhancing technology provides an excellent example of what can be achieved using a doubly-enabling, positive-sum approach which maximizes both goals – in this case, individual privacy *and* data quality.

Source: *Co-authored with Khaled El Emam, Ph.D. (Canada Research Chair in Electronic Health Information, CHEO Research Institute and University of Ottawa) – A Positive-Sum Paradigm in Action in the Health Sector, March 2010.*

5. **Maximizing Personal Privacy and the Benefits of Electronic Health Records (EHRs):** On the one hand, the transition from paper-based to electronic records can enable immediate access to large volumes of personal health information, often over great distances, which can vastly improve primary care and facilitate secondary uses. On the other hand, electronic systems pose unique risks to privacy and security, not least of all because information from diverse sources can be amassed and accessed in electronic format, by authorized users who may be far removed from the site of original collection. Information stored indefinitely in large-scale data repositories may more quickly and easily be linked to information from other data repositories, and may conceivably be used for an ever-increasing number of as-yet-undefined, future purposes. This paper begins with an overview of some of the elements already in place or under development, which form the basis of a framework to govern secondary use in the EHR environment. These existing measures include statutory safeguards, independent privacy oversight, and principles set out in a statement of Common Understandings, developed by the Pan-Canadian Health Information Privacy Group.

Source: *Richard C. Alvarez, Co-author (Canada Health Infoway) – Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/ Win, March 2012.*

6. **Privacy and Use of Home Health Care Technologies:** Written with Intel and GE, this paper helps us to understand these remote home health technologies and their uses. It identifies the privacy considerations, and provides an approach whereby privacy can be designed directly into these systems in a positive-sum manner, both protecting the personal data of individuals and maintaining the functionality and health benefits of the remote technologies being used.

Source: *Co-authored with David A. Hoffman (Intel), Scott Killen (GE) – Remote Home Health Care Technologies: How to Ensure Privacy? Build It In:* Privacy by Design*, November 2009.*

See also other co-authored papers: Alex Mihailidis, Ph.D., (University of Toronto), Jennifer Boger, (University of Toronto), Intelligent Assistive Technology and Systems Lab (IATSL) – *Sensors and In-Home Collection of Health Data: A* Privacy by Design *Approach, August 2010*; We Care, Medshare, Healthanywhere Inc., Research In Motion – *Innovative Wireless Home Care Services: Protecting Privacy and Personal Health Information, March 2009.*

7. **Protecting Smart Meter Consumer Energy Usage Data and Achieving Energy Efficiency, Conservation, Reliability and Sustainability Objectives:** Armed with an understanding of where privacy issues are likely to arise in the Smart Grid, regulators can help utilities understand privacy through the lens of a positive-sum, rather than a zero-sum, paradigm. When operating in this paradigm, utilities may believe that privacy interferes with other operational goals of the Smart Grid. Looking at privacy through the lens of a positive-sum paradigm, it becomes clear that a win-win situation is possible. The Smart Grid can achieve all of its objectives AND provide strong privacy for consumers. Indeed, designing privacy protections into the Smart Grid need not weaken security or functionality – it can, in fact, enhance the overall design of the system.

   Important factors for regulators to consider include:

   a) Understand – Are Smart Grid projects being planned in your jurisdiction? Which utility companies are involved? Who are the market leaders and what is their vision? Familiarize your office with the essentials.

   b) Engage – Find the key people involved with the Smart Grid in your local utilities. Determine their level of understanding, educate them and open a dialogue about privacy.

   c) Partner – Where appropriate, seek opportunities to develop white papers, best practices, and public FAQs in partnership with your local utilities. Recognize the popular myth that the utility can't implement privacy because their focus is on security (or functionality, or some other objective).

Source: *Shaping Privacy on the Smart Grid – You Can Make a Difference: A Roadmap for Data Protection Commissioners and Privacy Regulators, October 2010.*

Principle 5

End-to-End Security – *Full Lifecycle Protection*

Operational Guidance: *Security is the key to privacy. These actions ensure cradle-to-grave, lifecycle management of information, end-to-end, so that at the conclusion of the process, all data are securely destroyed, in a timely fashion.*

Actions	Responsibility
1. Employ encryption by default to mitigate the security concerns associated with the loss, theft or disposal of electronic devices such as laptops, tablets, smartphones, USB memory keys and other external media. The default state of data, if breached, must be "unreadable."	Software Engineers & Developers
2. Deploy encryption correctly and carefully integrate it into devices and workflows in an automatic and seamless manner.	Application & Program Owners
3. Ensure the secure destruction and disposal of personal information at the end of its lifecycle.	Line of Business & Process Owners

End-to-end security seeks the highest standard of data security possible. Organizations must assume responsibility for the security of personal information (including confidentiality, integrity and availability) throughout its entire lifecycle (at rest, in transit, while in use), consistent with the international standards that have been developed by recognized standards development organizations. Data security is essential to information privacy but does not equal privacy. Information security may be compared to a chain – it is only as strong as its weakest link.

Guidance on technical requirements for strong encryption – A health information example


Fact Sheet

Health-Care Requirement for Strong Encryption

a) Secure implementation – The encryption system should meet a minimum standard for the protection of sensitive information. This, in turn, has two components: encryption systems must be designed to meet a minimum standard; and encryption products should be independently validated against standards to ensure that they are designed and implemented properly. As explained below, the most suitable and widely used standard for encryption systems for mobile devices is FIPS 140-2 and this standard specifies only a few acceptable algorithms. Strong encryption requires the use of devices or software programs that are FIPS 140-2 certified for use in the way that they are designed to be operated.

b) Secure and managed encryption keys – Encryption keys must –

   a. be of a sufficient length (sometimes also called key size and measured in bits) that they effectively resist attempts to break the encryption; and

   b. remain protected so that they cannot be stolen or disclosed to unauthorized individuals.

c) Secure authentication of users – Prior to decrypting, authorized users must be securely authenticated (e.g., by means of robust passwords) to ensure that only authorized users can decrypt and access data.

d) No unintended creation of unencrypted data – No file containing decrypted data should persist because of a user having accessed encrypted data and viewed or updated it in decrypted form. A copy of the decrypted data must not persist unless an authorized user has intentionally created one.

In addition, the following are functional requirements of encryption systems that protect client privacy while at the same time supporting health-care providers in their ongoing provision of quality health care:

e) Identified, authorized and trained users – Health information custodians should be able to determine at any given time which users have access to encrypted information on a given mobile device or on mobile media. This means that users who are authorized to access or update encrypted data need to be individually identified beforehand and given appropriate authentication tokens (e.g., robust passwords), as well as adequate training in how to access and protect the encrypted information.

f) Encryption by default – Once an encryption system has been installed on a mobile device or to protect mobile media, users should be able to rely on the encryption being in place without having to explicitly activate it to protect data.

g) Availability and information lifecycle protection – There must be a reasonable assurance that encrypted data will remain available (e.g., despite forgotten passwords, staff who are unavailable due to illness or death, etc.). This, in turn, requires centralized management of passwords and other authentication tokens. It also requires that encrypted files or media be capable of being backed up along with other (unencrypted) files during routine backup operations.

All of the above considerations apply when encryption is used to secure the data stored on mobile devices and media such as laptops, cellphones, portable hard drives and memory sticks. They also apply to encryption used as an integral part of secure communications such as virtual private networks, secure email systems, and secure Web access. However, there is a final functional consideration when entire IT infrastructures are being designed and built:

h) Threat and Risk Assessment – IT infrastructures that use security technologies such as encryption should be subjected to a Threat and Risk Assessment prior to live operations (and preferably prior to implementation) to ensure that they work as expected.

Source: *Fact Sheet 16: Health-Care Requirement for Strong Encryption, July 2010.*

The following examples illustrate how this principle has been operationalized within other domains:

1. **Protecting Personal Data in Transit, by Default:** In 2009, my office called on Google to enable Secure Socket Layer (SSL) protections as the default option in Gmail. Today, the Gmail default setting is "Always use https." The presence of such 'designed-in' privacy features protects user privacy and heightens security, while allowing users to choose security settings, as they see fit.

Source: *If You Want To Protect Your Privacy, Secure Your Gmail, July 2009.*

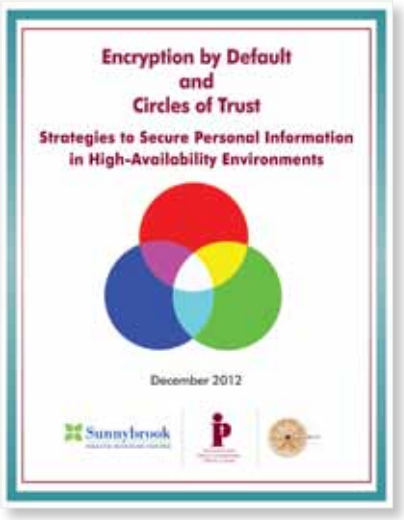
> *This is amazing. Every time I see something like this, it makes me sad that the U.S. doesn't have anything like your office. The Commissioner has yet again shown bold leadership in the privacy space. I can only hope that the major Web 2.0 companies listen to her, and embrace the philosophy of* Privacy By Design. *Pat yourselves on the back for doing a great job.*
>
> **Christopher Soghoian,**
> **formerly with Berkman Centre for Internet & Society,**
> **Harvard University**

2. In a Cloud Computing environment, a consumer (individual or enterprise) may choose to encrypt all personal or otherwise sensitive data both while the data is stored on a Cloud service provider's servers (at rest) and while being transmitted to end-users (in motion) – along with, of course, appropriate protections while the data is in use. Encrypting consumer data prior to outsourcing to the Cloud is at the heart of the architecture proposed in a Cloud Computing paper co-written with NEC, along with systems to ensure appropriate access to data is not reduced.

Source: *Co-authored with NEC Company Ltd. – Modelling Cloud Computing Architecture Without Compromising Privacy: A P*rivacy by Design *Approach, May 2010.*

3. **Analyzing Encrypted Data For Insights:** In a paper written for an IEEE conference on the Smart Grid, we proposed using what is known as a "Fully Homomorphic Encryption Scheme" that allows users to hand off the processing of data to a vendor without giving away access to that data. The technique adds an important layer of safety and privacy to the online world in settings ranging from banking and health care to networks and Cloud computing. This significant research was recognized by the IPC through the PET Symposium award for innovative research in privacy and security to Craig Gentry, IBM. The work of Dr. Khaled El Emam also involves a protocol that uses an additive homomorphic encryption system allowing mathematical operations to be performed on encrypted values. This is in conjunction to his continuing work on de-identification and health research data.

Sources: *Award winner's breakthrough efforts reveal how technology can lock-in privacy: Commissioner Ann Cavoukian, July 2010*; *to be published Ann Cavoukian & Klaus Kursawe – Implementing* Privacy by Design*: The Smart Meter Case. Paper presented at "the IEEE International Conference on Smart Grid Engineering (SGE'12)," Oshawa, Ontario and Khaled El Emam,et al – (2012) A secure distribution logistic regression protocol for the detection of rare adverse drug events, Journal of the American Medical Informatics Association.*



4. **Protecting Sensitive Data by Default in High Availability Environments:** *Encryption by Default and Circles of Trust* – This paper outlines strategies to secure personal information stored on portable storage media in high availability environments such as in a large, complex hospital environment. Circles of trust is a concept modeled after the Circle of Care concept and refers to mobile encryption deployment scenarios that enable free flow of personal health information among authorized health-care providers while at the same time, ensuring that the data remains, by default, inaccessible to anyone else. Encryption solutions (whether for data in motion or data at rest) can be applied either as an enterprise 'end point protection' or 'data loss protection' solution (e.g. as part of a

centralized security policy enforcement 'suite', which may also include port and plug-in device control with auto-encryption options) or as a stand-alone 'end point solution' applied on a case by case basis.

Source: *Co-authored with Jeff Curtis (Sunnybrook Health Sciences), Nandini Jolly (CryptoMill Technologies) – Encryption by Default and Circles of Trust, December 2012.*

5. **Removing Identity Data At Source:** Secure Visual Object Coding – This technology is introduced in the context of video surveillance and mass transit systems. Cryptographic techniques are used to secure a private object (personally identifiable information), so that it may only be viewed by designated persons of authority, by unlocking the encrypted object with a secret key. In other words, objects of interest (e.g., a face or body) are stored as completely separate entities from the background surveillance frame, and efficiently encrypted. This approach represents a significant technological breakthrough because by using a secure object-based coding approach, both the texture (i.e., content) and the shape of the object or just the texture may be encrypted.


Video Surveillance Cameras:
An Innovative Privacy-Enhancing Approach

Source: *Video Surveillance Cameras: An Innovative Privacy-Enhancing Approach, March 2008. [Based on the work of Karl Martin Ph.D., President & CEO, Bionym Inc., Toronto, Canada.]*

Guidance on Secure Destruction

Any organization, whether in the public or private sector, should follow responsible, secure procedures for the destruction of records containing personal information, once a decision has been made not to retain or archive this material. In many cases, it is not just a matter of being responsible, protecting one's reputation, or preventing identity theft – it may be a legal requirement.

Presented below are best practices for a secure destruction program:

- Organizations considering the destruction of records containing personal information should develop a secure destruction policy that determines in advance what records should be destroyed, by whom, and when.
- The policy should describe the destruction program, including details regarding methods of in-house or outsourced destruction, and contingency planning.
- Records to be destroyed should be segregated and securely stored throughout the entire process, before and after the destruction.

- In determining the method of destruction, organizations should consider the medium of the record, whether the records require a stronger method of destruction based on their sensitivity, and whether the media will be reused internally or moved out of the organization.
- Neither recycling records nor simply placing them in the trash are acceptable methods of destruction – avoid both.
- The destruction of records containing personal health information should be documented by way of internal authorizations prior to their destruction, and a Certificate of Destruction must be created once the destruction is completed.
- Before employing a service provider that will securely destroy all records, organizations should develop criteria for choosing a provider, as well as confirming the provider's methods of destruction and how records will be securely transported to the provider selected.
- Organizations should sign a contract or formal agreement with all external service providers hired to destroy records.
- Once materials are securely destroyed, they should be restricted from public access until disposed of permanently.
- Organizations should audit their secure destruction programs to ensure employee and service provider compliance.

Source: *Robert Johnson, Co-author (National Association for Information Destruction (NAID)) – Get rid of it Securely to keep it Private: Best Practices for the Secure Destruction of Personal Health Information, October 2009.*

Principle 6

Visibility and *Transparency* – Keep it *Open*

Operational Guidance: *Stakeholders must be assured that whatever the business practice or technology involved, it is, in fact, transparent to the user, and operating according to the stated promises and objectives, subject to independent verification.* ***Remember, trust but verify.***

Actions	Responsibility
1. Make the identity and contact information of the individual(s) responsible for privacy and security available to the public and well known within the organization.	Leadership/Senior Management
2. Implement a policy that requires all "public-facing" documents to be written in "plain language" that is easily understood by the individuals whose information is the subject of the policies and procedures.	Software Engineers
3. Make information about the policies, procedures and controls relating to the management of Personal Information readily available to all individuals.	Application Developers
4. Consider publishing summaries of PIAs, TRAs and independent, third party audit results.	Systems Architect
5. Make available a list of data holdings of Personal Information maintained by your organization.	
6. Make audit tools available so that users can easily determine how their data is stored, protected and used. Users should also be able to determine whether the policies are being properly enforced.	

Visibility and transparency are essential to establishing accountability and trust – not only for individuals but also for business partners, regulators and other involved stakeholders. It is increasingly in the interests of everyone – from application developers to systems architects, as well as organizational leadership – to be able to demonstrate effective privacy due diligence, especially in the event of a breach, a complaint, or an external audit. The long-term audit requirements imposed by FTC settlements are evidence of heightened expectations in this realm. Here in Ontario, personal health data registries must similarly sign affidavits every three years to confirm that they are adhering to minimum policies and practices.

You can outsource services, but you cannot outsource accountability. There are also growing demands for audit rights in contracts, and for concrete evidence of adherence to standards, contracts, and laws. Privacy metrics are essential. Standardized processes and third party privacy seals or marks of review, approval and certification may also be useful. In 2007, EuroPriSe introduced a European Privacy Seal for IT-products and IT-based services that have proven privacy compliant under European data protection laws in a two-step independent certification procedure. More recently, in October 2012, The Future of Privacy Forum and TRUSTe launched a Smart Grid Privacy Seal Program.

Current work by international data protection authorities to define accountability standards may also advance *Privacy by Design* practices. International standards groups are developing privacy assessment, control and implementation methodologies.

The implementation of *Privacy by Design* also opens up a stream of dialogue, not only within organizations, but also between organizations and the customers they serve. The importance of this dialogue cannot be overstated – effective communication with end-users is the essential link between implementing strong privacy practices and fostering the consumer confidence and trust that leads to sustainable competitive advantage. Further, it enables privacy leaders to earn the recognition they deserve.

For this reason, it is essential that important privacy attributes about a system or process be brought to users' attention in relevant, timely and actionable ways. It should be relatively simple for users to find out critical privacy details about a technology or information system and how it operates. Clear documentation that is easily understood and that provides a reasonable and sufficient basis for informed decision-making must be provided.

There is widespread consensus that the prevailing Notice and Choice approach to user privacy is deeply flawed. Users rarely read the lengthy and legalistic "take it or leave it" policies and terms they are often presented with. Organizations that rely on such policies are mistaken if they believe that consumers have seen, understood or knowledgably accepted their privacy practices.

Whether installing a new application, or interacting with a website and social networking platform, users need to be well informed about important system privacy attributes, including, at a minimum, what privacy policies apply and who is responsible for them.

In applying this principle, it is useful to bear in mind that the way we interact with devices is constantly changing. Considerable research and experimentation is being undertaken into Human-Computer Interface (HCI) design to improve user awareness and understanding. Other

potentially relevant approaches that are being explored include standardized short notices and machine-readable privacy policies.

The following provide examples of how this principle is implemented. Also, refer to the accountability tools and examples provided under Principle 1: "***Proactive*** not Reactive; ***Preventative*** not Remedial."

Guidance on Visibility and Transparency: CCTV/Video Surveillance and RFID programs

CCTV/Video Surveillance

- The public should be notified, using clearly written signs, prominently displayed at the perimeter of the video surveillance areas of video surveillance equipment locations, so the public has reasonable and adequate warning that surveillance is, or may be in operation, before entering any area under video surveillance. Signs at the perimeter of the surveillance areas should identify someone who can answer questions about the video surveillance system, and can include an address, telephone number, or website for contact purposes.
- Organizations should be as open as possible about the video surveillance program in operation and upon request, should make available to the public information on the rationale for the video surveillance program, its objectives and the policies and procedures that have been put in place. This may be done in pamphlet or leaflet form. A description of the program on an organization's website would also be an effective way of disseminating this information.
- Organizations should ensure that the use and security of video surveillance equipment is subject to regular audits. The audit should also address the organization's compliance with the operational policies and procedures. An external body may be retained in order to perform the audit. Any deficiencies or concerns identified by the audit must be addressed immediately.
    - In the 2008 TTC Privacy Investigation Report (MC07-68) one of the recommendations pertains to audits ("The TTC must ensure that its video surveillance program is subjected to an effective and thorough audit conducted by an independent third party, using the *GAPP Privacy Framework*.")

Source: *Guidelines for the Use of Video Surveillance Cameras in Public Places, September 2007.*

Radio Frequency Identification (RFID)

Accountability: An organization is responsible for personal information under its control and should designate a person who will be accountable for the organization's compliance with the following principles, and the necessary training of all employees. Organizations should use contractual and other means to provide a comparable level of protection if the information is disclosed to third parties. Organizations that typically have the most direct contact and primary relationship with the individual should bear the strongest responsibility for ensuring privacy and security, regardless of where the RFID-tagged items originate or end up in the product lifecycle.

Openness:

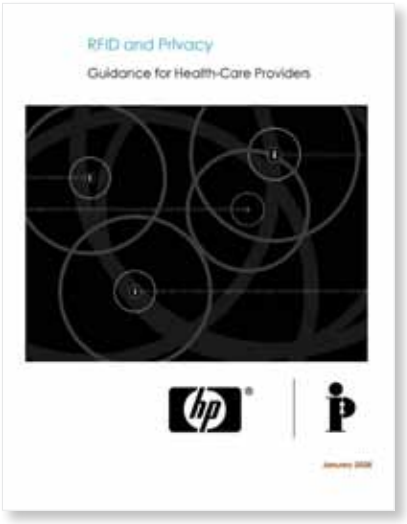
- Organizations should publish, in compliance with applicable laws, information on their policies respecting the collection, retention, and uses of RFID-linked consumer information.
- Organizations should make available to the public general information about the RFID technology in use and the meaning of all symbols and logos used.
- Organizations should notify consumers if products contain an RFID tag, through clear and conspicuous labelling on the product itself.
- Organizations should notify consumers of RFID readers on their premises, using clearly written signage, prominently displayed at the perimeter.
- Signs at the perimeter should identify someone who can answer questions about the RFID system, and include their contact information.
- Consumers should always know when, where, and why an RFID tag is being read. Visual or audio indicators should be built into the operation of the RFID system for these purposes.

Challenging Compliance:

- Organizations should inform consumers of their rights and available procedures to challenge that business' compliance with these privacy principles.
- Organizations may wish to ensure that the use and security of any RFID technology or system is subject to regular audits. For example, the audit could address the company's compliance with the operational policies and procedures.

Source: *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines), June 2006.*

For application of these guidelines to the health sector, see *RFID and Privacy: Guidance for Health-Care Providers*, January 2008. The essential purpose of this publication is to assist the health-care sector in understanding the current and potential applications of RFID technology, its potential benefits, privacy implications, and the steps that can be taken to mitigate potential threats to privacy.



Source: *Co-authored with Victor Garcia, Hewlett-Packard (HP) – RFID and Privacy: Guidance for Health-Care Providers, January 2008.*

Short Notices to the Public under the *Personal Health Information Protection Act*

In 2005, in response to repeated requests from the health sector for short, easy-to-understand notices to the public about the *Act*, the IPC developed a set of short notices to help health information custodians carry out their responsibilities under the *Act*. In conjunction with the Ontario Bar Association (Privacy and Health Law sections), the Ministry of Health and Long-Term Care and the Ontario Dental Association, the IPC developed short notices to inform the public about the information practices of health-care custodians. These short notices can be used by health-care providers (*In Our Office*), hospitals (*In Our Hospital*), and long-term care facilities (*In Our Facility*).

Source: *Short Notices to the Public under the Personal Health Information Protection Act: Your Health Information and Your Privacy in Our Office; Your Health Information and Your Privacy in Our Hospital; Your Health Information and Your Privacy in Our Facility, June 2005.*

Principle 7

Respect for User Privacy – Keep it *User-Centric*

Operational Guidance: *This method 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.***

Actions	Responsibility
1. Offer strong privacy defaults. 2. Provide appropriate notice. 3. Consider user-friendly options: a. Make user preferences persistent and effective. b. Provide users with access to data about themselves. c. Provide access to the information management practices of the organization.	Leadership/Senior Management Software Engineers & Developers Application & Program Owners Line of Business & Process Owners

At its core, respecting the user means that when designing or deploying an information system, an individual's privacy and user interests are accommodated, right from the outset. User-centricity is designing for the user, anticipating his or her privacy perceptions, needs, requirements, and default settings.

Operational aspects of this principle include measures to assure transparency, attain informed user consent, provide rights of access and correction, and make effective redress mechanisms available. Users expect privacy preferences and settings to be clear, to function across platforms, and to persist over time. Preferences and settings should also cascade to third parties (e.g. opt-out). Robust consent mechanisms have significant uses in the Cloud, social and mobile computing applications, online tracking and advertising services, online contracts, electronic health records, and personal data vaults. These issues are being examined by industry and public policy-makers. Organizational policies and processes should demonstrate the same degree of consideration for users at all touch points and interactions.

There must be a way for users to gain insight into the operations and functioning of any technology or system that they are interacting with, preferably in real time. User controls should be timely and actionable, and supported by appropriate feedback. Defaults should be set appropriately, by which we mean in the most privacy-protective manner possible.

The concept of "user-centricity" has evolved into two sometimes contradictory meanings in networked or online environments. As it pertains to privacy, it contemplates a right of control by an individual over his or her personal information when online, usually with the help of technology. For most system designers, however, it describes an information and communications system built with users in mind, which anticipates and addresses their privacy interests, risks and needs. One view is libertarian (informational self-determination); the other is somewhat paternalistic. Both views are valid, but must be qualified in the Information Age. *Privacy by Design* embraces both understandings of user-centricity. Information technologies, processes and infrastructures must be designed not only *for* individual users, but also *structured by them*. Users are rarely, if ever, involved in every design decision or transaction involving their personal information, but they are nonetheless in an unprecedented position today to exercise a measure of meaningful control over those designs and transactions, as well as the disposition and use of their personal information by others. As with the other principles of Fair Information Practices and *Privacy by Design*, Respect for User Privacy is not a stand-alone principle. It is intertwined with the remaining principles (e.g., on transparency, security safeguards, default settings, embedding privacy, and achieving positive-sum results).

The long-standing privacy principle of individual access is intended as a transparency-enhancing check against abuses, and inaccuracies, either by the state or the private sector. Empowering users to play active roles in the management of their personal data may be the single most effective check against abuses and misuses. "The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard." The OECD Guidelines go on to note that "The right to access should, as a rule, be simple to exercise" and be subject to as few exceptions as possible. The concept relating to online access and security was the focus of a U.S. Federal Trade Commission committee report issued in 2000. As such, this *PbD* Principle has important links to the field

of user interface design. The user interface is that dimension of the system by which users interact with a machine. It includes hardware (physical) and software (logical) components.

Individual access rights are enshrined in most public sector privacy laws and practices. Today, an access revolution has been occurring in Cloud, mobile and social computing contexts. Online account management is common, and people expect direct access to personal data held about them, especially when there is a privacy breach.

In this spirit, my office applauded the launch of Google Dashboard, which gave users unprecedented visibility, insight and control into the collection, use and disclosure of their personal information across Google's services. Indeed, generally speaking, we have been supportive of any user-controlled devices, agents, and platforms that allows maximum user control over personal data and its processing by others, such as personal health records, data vaults, and ultimately SmartData.

The following are examples of mechanisms that take a user-centric approach to privacy:

1. **Making e-Government Citizen-Centric:** Individual participation and control enabled by Web 2.0 technology and applications. An example of how this principle may be operationalized is through modern technologies that make it feasible, on a scale never before imagined, to allow citizens to directly access information held about them, to learn of its uses, and to play a more direct role in the care and management of this data – allowing them to review and edit their data, to set preferences, to direct uses, and to learn how their data has been disclosed and used. Empowered citizens are ones who can fully exercise informational self-determination, that is, the ability to exercise control over the collection, use and disclosure of their personal information.

Source: *Privacy and Government 2.0: The Implications of an Open World, May 2009.*

2. **Building Privacy into User Interface Design:** Through this joint paper with Yahoo!, we contributed to a deepening evidence base that the privacy and policy community can draw upon in future work that exemplifies user-centricity. Good product and business process designs are needed to empower users to achieve strong privacy. Effective user interfaces are critical to good design and operation. General user interface (UI) or user experience (UX) design ("UID/UXD") theory and evaluation criteria continue to evolve with 21st century technologies. The application of UI/UX design principles to the online environment and user privacy experience represents a subset of a much larger field of inquiry. Context matters greatly in how design principles and criteria are applied. Legal requirements, project domain and scope, objectives to be achieved, and the nature, volume and sensitivity of the personal data processing involved will all vary in influence, along with the extent of user participation. Context must inform sound decision-making, and must therefore be the cornerstone of sound design. Adaptation to a privacy context requires taking a principled approach, executing judgement, and considering some form of metrics.

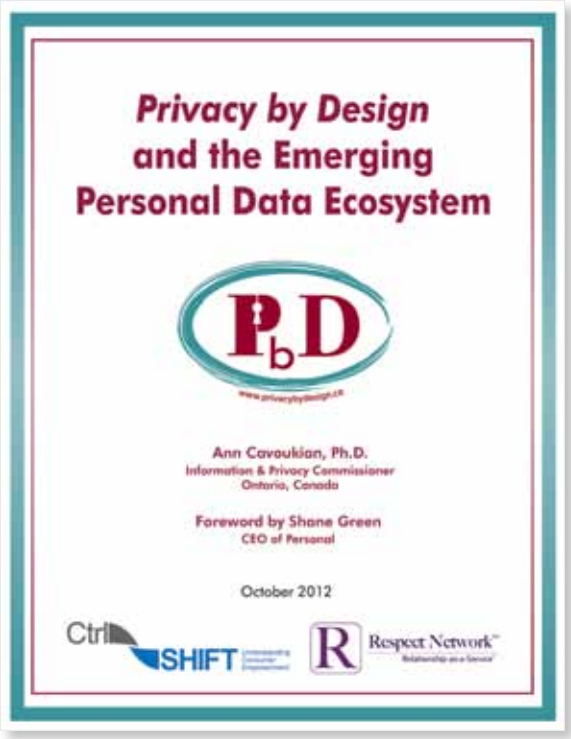
Source: *Justin B. Weiss, Co-author (Yahoo!)* – Privacy by Design *and User Interfaces: Emerging Design Criteria - Keep it User-Centric, June 2012.*

3. **Creating a User-centric Identity Management MetaSystem:** The goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of sharing their information will be. In other words, these tools should enable users to give informed consent. The default should be minimal disclosure, for a defined purpose. Any secondary or additional use should be optional after enrolment.

   This means that the identity infrastructure must account for many devices, from desktop PCs to mobile phones. The infrastructure must allow for a unified user experience spanning widely over all devices. It also means that the system must be driven throughout by a clear framework of agreed-upon rules. This includes policies describing to users what information is requested and why (similar to a machine-readable and improved version of today's privacy policies). It must also include a "sticky" policy that travels with the information throughout its lifetime and ensures that it is only used in accordance with the policy. The last step will of course require mechanisms to enforce these sticky policies in ways that can be verified and audited.

Source: *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age, October 2006. [Based on the "7 Laws of Identity" formulated through the leadership of Kim Cameron, Identity Architect, Microsoft]*

4. **Engineering Personal Control of Online Data:** Personal Data Vaults and the Emerging Personal Data Ecosystem. The rise of the Personal Data Ecosystem (PDE) can be viewed as the biggest leap forward for personal privacy on the Internet since the advent of the privacy policy. There are game changing systems and initiatives that seek to address the challenge of protecting and promoting privacy, while at the same time, encouraging socio-economic opportunities and benefits. Within a PDE, individuals have: a) more explicit control over the sharing of their personal data online, and b) new trust frameworks that raise the collective expectation of how companies and organizations will respect an individual's right to control his or her personal data. The PDE is the ultimate in user-centric design!

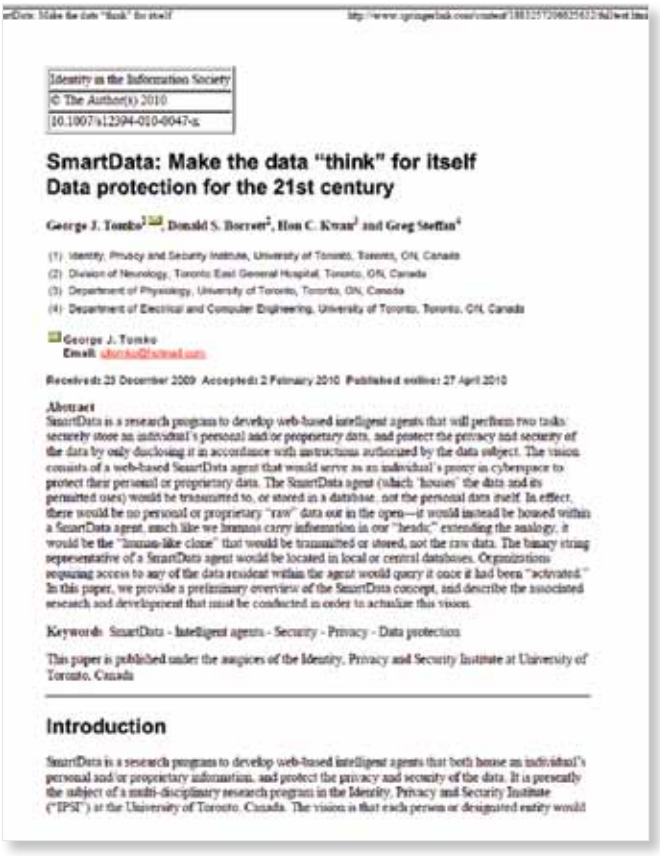


Source: *Co-authored with Shane Green, Josh Galper (Personal), Drummond Reed (Respect Network), Liz Brandt, Alan Mitchell (Ctrl-Shift),* – Privacy by Design *and the Emerging Personal Data Ecosystem, October 2012.*

HOT DOC: ONE PRIVACY PAPER TO READ THIS WEEK – *Washington is obsessed with the concept of "*privacy by design*" – it's in the FTC's privacy report, it guides the White House's online privacy blueprint and it's proven infectious on Capitol Hill. But the mind behind the idea – Dr. Ann Cavoukian, the top privacy cop in Ontario, Canada – is out with a new report today that points out the intersection of "*privacy by design*" with personal data vaults, and similar technologies – an industry segment that's starting to explode.*

Politico's Morning Tech, October 31, 2012

5. **SmartData. Privacy Meets Evolutionary Robotics:** Protecting Freedom Using Virtual Tools. Technology must form an integral component in the defence of our personal privacy. Policies and regulations will serve, at best, as lagging remedies in the fast-paced world of cyberspace. In a world where personal information can increasingly be transmitted and used in multiple locations simultaneously, protecting privacy may only truly be accomplished if the information itself becomes "intelligent" and capable of making appropriate decisions, relating to its release, on behalf of the data-subject. In other words, the data must become "smart" – hence, we need SmartData. This research at the Identity, Privacy and Security Institute at the University of Toronto looks into the growing need, the challenges, and ultimately, the benefits of developing virtual, intelligent agents to protect our privacy online.



Identity in the Information Society
© The Author(s) 2010
10.1007/s12394-010-0047-x

SmartData: Make the data "think" for itself
Data protection for the 21st century

George J. Tomko[1], Donald S. Borrett[2], Hon C. Kwan[3] and Greg Steffan[4]

(1) Identity, Privacy and Security Institute, University of Toronto, Toronto, ON, Canada
(2) Division of Neurology, Toronto East General Hospital, Toronto, ON, Canada
(3) Department of Physiology, University of Toronto, Toronto, ON, Canada
(4) Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada

George J. Tomko
Email: [redacted]

Received: 23 December 2009 Accepted: 2 February 2010 Published online: 27 April 2010

Abstract
SmartData is a research program to develop web-based intelligent agents that will perform two tasks: securely store an individual's personal and/or proprietary data, and protect the privacy and security of the data by only disclosing it in accordance with instructions authorized by the data subject. The vision consists of a web-based SmartData agent that would serve as an individual's proxy in cyberspace to protect their personal or proprietary data. The SmartData agent (which 'houses' the data and its permitted uses) would be transmitted to, or stored in a database, not the personal data itself. In effect, there would be no personal or proprietary "raw" data out in the open—it would instead be housed within a SmartData agent, much like we humans carry information in our "heads," extending the analogy, it would be the "human-like clone" that would be transmitted or stored, not the raw data. The binary string representative of a SmartData agent would be located in local or central databases. Organizations requiring access to any of the data resident within the agent would query it once it had been "activated." In this paper, we provide a preliminary overview of the SmartData concept, and describe the associated research and development that must be conducted in order to actualize this vision.

Keywords SmartData - Intelligent agents - Security - Privacy - Data protection

This paper is published under the auspices of the Identity, Privacy and Security Institute at University of Toronto, Canada

Introduction

SmartData is a research program to develop web-based intelligent agents that both house an individual's personal and/or proprietary information, and protect the privacy and security of the data. It is presently the subject of a multi-disciplinary research program in the Identity, Privacy and Security Institute ("IPSI") at the University of Toronto, Canada. The vision is that each person or designated entity would

Source: George *Tomko, Ph.D., Donald Borrett, Ph.D., Hon C. Kwan, Ph.D., & Greg Steffan, Ph.D., SmartData: Make the data "think" for itself. Data Protection for the 21st Century, February 2010.*

Conclusions

This paper provided an overview of some of the work that my office has been engaged in over the years, and the experiences of our innovative partners in these efforts to give meaningful operational effect to the principles of *Privacy by Design*. By reflecting on the work of many international companies and organizations, I hope to encourage readers to create their own paths.

Our work is far from complete – in fact, it has just begun. There is a long road ahead in the journey of translating *PbD*'s 7 Foundational Principles into concrete, prescriptive requirements, specifications, standards, best practices, and operational performance criteria. It is a journey that must, by necessity, involve not only executives, but especially software engineers and designers, risk managers, marketing and customer service professionals, legal departments, project managers, privacy officers, and many others. It must also encompass business requirements, engineering specifications, development methodologies, and security controls, according to each domain or project scope.

There are already a number of initiatives underway that represent the concrete steps taken toward operationalizing *PbD* and making its implementation part of the default rules for the next generation of privacy advocates who will be tasked with responding to the new challenges we will face. One exciting development is a new Technical Committee of the international standards body OASIS (the Organization for the Advancement of Structured Information Standards) – *PbD*-SE (Software Engineers), to develop and promote standards for *PbD* in software engineering, that I am co-chairing with Dr. Dawn Jutla, a professor of engineering at St. Mary's University, Nova Scotia. She is the winner of the prestigious U.S. World Technology Award (IT Software – Individual 2009) and is recognized for her innovative work with long-term significance on the evolving technological landscape as well as the transcendent imperative of privacy protection. At Carnegie Mellon University, Professors Lorrie Faith Cranor and Norman Sadeh have developed a new graduate program combining engineering and privacy – a Master's program in "Privacy Engineering." A major element of the program is a *PbD* "learn-by-doing" component.

As I mentioned at the outset of this paper, the exercise of operationalizing *Privacy by Design* – taking it from principles to actions – is one that each organization will undertake in its own way. It is my hope that as they do so, they will make their own stories – their challenges, victories, and lessons learned – broadly available so that the privacy community may continue to build much-needed expertise, and grow best practices, for the benefit of all. I have always said that *Privacy by Design* is not a theoretical construct or academic formulation – it has to have legs, on the ground, now, in order to be effective. Together, we can make the concept of privacy a reality, by design – now, and well into the future.

Appendices

Privacy by Design Papers Organized by Application Area

CCTV/Surveillance Cameras in Mass Transit Systems

- *Guidelines for the Use of Video Surveillance Cameras in Public Places*, Dr. Ann Cavoukian, September 2007. http://www.ipc.on.ca/images/Resources/video-e.pdf
- *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report*, Dr. Ann Cavoukian, March 2008. http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf

Biometrics Used in Casinos and Gaming Facilities

- *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, Dr. Ann Cavoukian & Alex Stoianov, Ph.D., March 2007. http://www.ipc.on.ca/images/Resources/bio-encryp.pdf
- *The Relevance of Untraceable Biometrics and Biometric Encryption: A Discussion of Biometrics for Authentication Purposes*, Office of the Information & Privacy Commissioner of Ontario and European Biometrics Group, August 2009. http://www.ipc.on.ca/images/Resources/untraceable-be.pdf
- *Biometric Encryption Chapter from the Encyclopedia of Biometrics*, Dr. Ann Cavoukian and Alex Stoianov, Ph.D., December 2009. http://www.ipc.on.ca/images/Resources/bio-encrypt-chp.pdf
- *Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept*, Office of the Information & Privacy Commissioner and Ontario Lottery and Gaming Corporation, November 2010. http://www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf
- *Fingerprint Biometric Systems: Ask the Right Questions Before You Deploy*, Dr. Ann Cavoukian, July 2008. http://www.ipc.on.ca/images/Resources/fingerprint-biosys.pdf
- *Fingerprint Biometrics: Address Privacy Before Deployment*, Dr. Ann Cavoukian, November 2008. http://www.ipc.on.ca/images/Resources/fingerprint-biosys-priv.pdf

Smart Meters and the Smart Grid

- *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation,* Office of the Information & Privacy Commissioner and the Future of Privacy Forum, November 2009. http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf
- *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid,* Office of the Information & Privacy Commissioner, Hydro One Networks and Toronto Hydro Corp., June 2010. http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf
- *Frequently Asked Questions – Smart Grid Privacy – From Smart Meters to the Future,* Dr. Ann Cavoukian, October 2010. http://www.ipc.on.ca/images/Resources/smartgrid-faq.pdf
- *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study,* Office of the Information & Privacy Commissioner, Hydro One, GE, IBM and Telvent, February 2011. http://www.ipc.on.ca/images/Resources/pbd-ont-smartgrid-casestudy.pdf
- *Applying Privacy by Design Best Practices to SDG&E's Smart Pricing Program,* Office of the Information & Privacy Commissioner and San Diego Gas & Electric, March 2012. http://www.ipc.on.ca/images/Resources/pbd-sdge.pdf
- *Smart Meters in Europe: Privacy by Design at its Best,* Dr. Ann Cavoukian, April 2012. http://www.ipc.on.ca/images/Resources/pbd-smartmeters-europe.pdf
- *Building Privacy into Ontario's Smart Meter Data Management System: A Control Framework,* Office of the Information & Privacy Commissioner and the Independent Electricity System Operator, May 2012. http://www.ipc.on.ca/images/Resources/pbd-ieso.pdf
- *Shaping Privacy on the Smart Grid – You can Make a Difference: A Roadmap for Data Protection Commissioners and Privacy Regulators,* Dr. Ann Cavoukian, October 2010. http://www.privacybydesign.ca/content/uploads/2010/10/2010-10-roadmap_brochure.pdf
- *Smart Grid Privacy 101: A Primer for Regulators,* Dr. Ann Cavoukian, October 2010. http://www.privacybydesign.ca/content/uploads/2010/10/smart-grid-primer.pdf
- *Embedding Privacy into Smart Grid Initiatives*, Dr. Ann Cavoukian, October 2010. http://www.privacybydesign.ca/content/uploads/2010/10/smartgrid-tipsheet.pdf

Mobile Devices & Communications

- *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users,* Dr. Ann Cavoukian and Professor Marilyn Prosch, December 2010. http://www.ipc.on.ca/images/Resources/pbd-asu-mobile.pdf

- *Wi-Fi Positioning Systems: Beware of Unintended Consequences,* Dr. Ann Cavoukian and Kim Cameron, June 2011. http://www.ipc.on.ca/images/Resources/wi-fi.pdf
- *Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes,* Office of the Information & Privacy Commissioner and the Children's Hospital of Eastern Ontario, September 2011. http://www.ipc.on.ca/images/Resources/cheo-mobile_device_research.pdf

Near Field Communications (NFC)

- Mobile Near Field Communications (NFC) 'Tap 'n Go' Keep it Secure and Private. Dr. Ann Cavoukian, November 2011. http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf

RFIDs and Sensor Technologies

- *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines),* Dr. Ann Cavoukian, June 2006. http://www.ipc.on.ca/images/Resources/rfid-guides&tips.pdf
- *Practical Tips for Implementing RFID Privacy Guidelines*, Office of the Information & Privacy Commissioner, June 2006. http://www.ipc.on.ca/images/Resources/up-rfidtips.pdf
- *RFID and Privacy – Guidance for Health-Care Providers*, Office of the Information & Privacy Commissioner and Hewlett-Packard Canada, January 2008. http://www.ipc.on.ca/images/Resources/rfid-HealthCare.pdf
- *Adding an On/Off Device to Activate the RFID in Enhanced Driver's Licenses,* Dr. Ann Cavoukian, March 2009. http://www.ipc.on.ca/images/Resources/edl.pdf

Redesigning IP Geolocation Data

- *Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising,* Office of the Information & Privacy Commissioner and Bering Media, October 2010. http://www.ipc.on.ca/images/Resources/pbd-ip-geo.pdf

Remote Home Health Care

- *Innovative Wireless Home Care Services: Protecting Privacy and Personal Health Information,* Office of the Information & Privacy Commissioner, March 2009. http://www.ipc.on.ca/images/Resources/wirelesshomecare.pdf
- *Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design,* Office of the Information & Privacy Commissioner, Intel and GE Healthcare, November 2009. http://www.ipc.on.ca/images/Resources/pbd-remotehomehealthcarew_Intel_GE.pdf
- *Fact Sheet / 16 – Health-Care Requirement for Strong Encryption*, Dr. Ann Cavoukian, July 2010. http://www.ipc.on.ca/images/Resources/fact-16-e.pdf

- *Sensors and In-Home Collection of Health Data: A Privacy by Design Approach,* Office of the Information & Privacy Commissioner and the Intelligent Assistive Technology and Systems Lab, August 2010. http://www.ipc.on.ca/images/Resources/pbd-sensor-in-home.pdf

Big Data and Data Analytics

- *Privacy by Design in the Age of Big Data,* Dr. Ann Cavoukian and Jeff Jonas, June 2012. http://www.ipc.on.ca/images/Resources/pbd-big_data.pdf

Foundational *PbD* Papers

- *Creation of a Global Privacy Standard,* Dr. Ann Cavoukian, November 2006. http://www.ipc.on.ca/images/Resources/gps.pdf
- *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum*, Dr. Ann Cavoukian, July 2008. http://www.ipc.on.ca/images/Resources/trans-tech.pdf
- *Privacy by Design*, Dr. Ann Cavoukian, January 2009. http://www.ipc.on.ca/images/Resources/privacybydesign.pdf
- *Moving Forward from PETs to PETs Plus: The Time for Change is Now,* Dr. Ann Cavoukian, January 2009. http://www.ipc.on.ca/images/Resources/petsplus_3.pdf
- *Privacy by Design: The 7 Foundational Principles,* Dr. Ann Cavoukian, August 2009. http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=883
- *Privacy by Design – The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices,* Dr. Ann Cavoukian, May 2010. http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf
- *Privacy by ReDesign: Building a Better Legacy,* Dr. Ann Cavoukian and Professor Marilyn Prosch, May 2011. http://www.ipc.on.ca/images/Resources/AVAwhite6.pdf
- *Privacy by ReDesign: A Practical Framework for Implementation,* Dr. Ann Cavoukian and Claudiu Popa, November 2011. http://www.ipc.on.ca/images/Resources/PbRD-framework.pdf
- *Privacy by Design Curriculum v2.0*, Dr. Ann Cavoukian, November 2011. http://privacybydesign.ca/publications/

Privacy by Design Papers Organized by Principle

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

- Cavoukian, Ann, *Building Privacy into Ontario's Smart Meter Data Management System: A Control Framework* (Office of the Information and Privacy Commissioner, Ontario, Canada and Ontario, May 2012), www.ipc.on.ca/images/Resources/pbd-ieso.pdf
- Cavoukian, Ann, Prosch, Marilyn. *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users* (Office of the Information and Privacy Commissioner, Ontario, Canada, December 2010), http://www.ipc.on.ca/images/Resources/pbd-asu-mobile.pdf
- Cavoukian, Ann, *Mobile Near Field Communications (NFC) "Tap 'n Go" - Keep it Secure and Private* (Office of the Information and Privacy Commissioner, Ontario, Canada, November 2011) http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf
- Cavoukian, Ann, *Privacy and Boards of Directors: What You Don't Know Can Hurt You* (Office of the Information and Privacy Commissioner, Ontario, Canada, November 2003), http://www.ipc.on.ca/images/Resources/director.pdf
- *A Policy is Not Enough: It Must be Reflected in Concrete Practices* (Office of the Information and Privacy Commissioner, Ontario, Canada, September 2012), http://www.ipc.on.ca/images/Resources/pbd-policy-not-enough.pdf
- Jesselon, Pat. & Fineberg, Anita. *The Privacy by Design Privacy Impact Assessment (The PbD-PIA),* (Office of the Information and Privacy Commissioner, Ontario, Canada, April 2011), http://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf
- Cavoukian, Ann, *The New Federated Privacy Impact Assessment (F-PIA) Building Privacy and Trust-enabled Federation* (Office of the Information and Privacy Commissioner, Ontario, Canada, January 2009), http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=836
- Wright, D., & de Hert, P. (2012). *Privacy Impact Assessment. Law, Governance and Technology Services*, Vol 6.
- Cavoukian, Ann., Abrams, E. Martin, Taylor, Scott., *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices* (Office of the Information and Privacy Commissioner, Ontario, Canada, November 2009), http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf
- Cavoukian, Ann, OLG, YMCA, *Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default* (Office of the Information and Privacy Commissioner, Ontario, Canada, April 2010), http://www.privacybydesign.ca/publications/accountable-business-practices/

- Office of the Information and Privacy Commissioner of Ontario and IBM, *Privacy by Design: From Policy to Practice* (Office of the Information and Privacy Commissioner, Ontario, Canada, September 2011), http://www.ipc.on.ca/images/Resources/pbd-policy-practice.pdf
- McQuay, Terry., Cavoukain, Ann, *A Pragmatic Approach to Privacy Risk Optimization: Privacy by Design for Business* (NYMITY and the Office of the Information and Privacy Commissioner, August 2009), http://privacybydesign.ca/?s=a+pragmatic+approach+to+privacy+risk+optimization

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

- Cavoukian, Ann, *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study* (Office of the Information and Privacy Commissioner, Ontario, Canada, February 2011), http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1037
- Cavoukian, Ann. *Adding an On/Off Device to Activate the RFID in Enhanced Driver's Licences: Pioneering a Made-in-Ontario Transformative Technology that Delivers Both Privacy and Security* (Office of the Information and Privacy Commissioner, Ontario, Canada, March 2009), http://www.ipc.on.ca/images/Resources/edl.pdf
- Office of the Information and Privacy Commissioner Ontario, *Video: A Word about RFIDs and Your Privacy in the Retail Sector.* (Office of the Information and Privacy Commissioner, Ontario, Canada, March, 2006), http://www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=663
- Cavoukian, Ann, *Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising* (Office of the Information and Privacy Commissioner, Ontario, Canada, Oct 2010), www.ipc.on.ca/images/Resources/pbd-ip-geo.pdf
- Cavoukian, Ann., El Emam, Khaled. *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy* (Office of the Information and Privacy Commissioner, Ontario, Canada, June 2011), www.ipc.on.ca/images/Resources/anonymization.pdf
- Cavoukian, Ann., El Emam, Khaled, *A Positive-Sum Paradigm in Action in the Health Sector* (Office of the Information and Privacy Commissioner, Ontario, Canada, March 2010), http://www.ipc.on.ca/images/Resources/positive-sum-khalid.pdf
- Cavoukian, Ann, *White Paper: Anonymous Video Analytics (AVA) technology and privacy* (Office of the Information and Privacy Commissioner, Ontario, Canada, April 2011), www.ipc.on.ca/images/Resources/AVAwhite6.pdf
- Cavoukian, Ann., Stoianov, Alex, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (Office of the Information and Privacy Commissioner, Ontario, Canada, March 2007), www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=608

- Cavoukian, Ann, *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum.* (Office of the Information and Privacy Commissioner, Ontario, Canada, July 2008), http://www.ipc.on.ca/images/Resources/trans-tech-handout_098824173750.pdf

- McDougall, P. (August 8, 2012). Microsoft IE 10 Makes 'Do Not Track' Default, InformationWeek.

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

- To be published Cavoukian, Ann., & Kursawe, Klaus. (2012). *Implementing Privacy by Design: The Smart Meter Case.* Paper presented at "the IEEE International Conference on Smart Grid Engineering (SGE'12)," Oshawa, Ontario

- Cavoukian, Ann., & Winn, Caroline., *Applying Privacy by Design Best Practices to SDG&E's Smart Pricing Program* (Office of the Information and Privacy Commissioner Ontario, Canada, March 2012), http://www.ipc.on.ca/images/Resources/pbd-sdge.pdf

- Rannenberg, K. (2010) *Privacy by Design in Mobile Applications and Location Based Services.* Paper presented at "*Privacy by Design*: The Gold Standard," Toronto, Ontario http://www.privacybydesign.ca/content/uploads/2010/03/PbD_in_Mobile_Applications_and_Location_Based_Services.20100128.Rannenberg.20100127.2.pdf

- Cavoukian, Ann, Prosch, Marilyn. *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users* (Office of the Information and Privacy Commissioner, Ontario, Canada, December 2010), http://www.ipc.on.ca/images/Resources/pbd-asu-mobile.pdf

- Cavoukian, Ann, *Mobile Near Field Communications (NFC) "Tap 'n Go" - Keep it Secure and Private* (Office of the Information and Privacy Commissioner, Ontario, Canada, November 2011) http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf

- Cavoukian, Ann., Jonas, Jeff. *Privacy by Design in the Age of Big Data* (Office of the Information and Privacy Commissioner, Ontario, Canada, June 2012), www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1195

- Cavoukian, Ann., & Cameron, Kim. *Wi-Fi Positioning Systems: Beware of Unintended Consequences* (Office of the Information and Privacy Commissioner, Ontario, Canada, June 2011) http://www.ipc.on.ca/images/Resources/wi-fi.pdf

- Cavoukian, Ann, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers* (Office of the Information and Privacy Commissioner, Ontario, Canada, Aug 2011) http://www.ipc.on.ca/images/Resources/pbd-law-policy.pdf

- Jean Camp, L. (2010) Respect by Design. *Paper presented at "Privacy by Design: The Gold Standard," Toronto, Ontario* http://www.privacybydesign.ca/content/uploads/2010/03/PrivacyByDesign1_28_test.pdf

- Federal Trade Commission, (2012) *Protecting Consumer Privacy in an Era of Rapid Change*, ftc.gov/os/2012/03/120326privacyreport.pdf p. 53

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

- Cavoukian, Ann. *Guidelines for the Use of Video Surveillance Cameras in Public Places* (Office of the Information and Privacy Commissioner, Ontario, Canada, September 2007), http://www.ipc.on.ca/images/Resources/video-e.pdf
- Cavoukian, Ann, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report MC07-68*, (Office of the Information and Privacy Commissioner, Ontario, Canada, March 2008), http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf
- Cavoukian, Ann., Marinelli, Tom. *Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept* (Office of the Information and Privacy Commissioner, Ontario, Canada, November 2010), www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf
- Office of the Information & Privacy Commissioner of Ontario, *Shaping Privacy on the Smart Grid - You Can Make a Difference: A Roadmap for Data Protection Commissioners and Privacy Regulators (*Office of the Information and Privacy Commissioner, Ontario, Canada, October 2010), http://www.privacybydesign.ca/content/uploads/2010/10/2010-10-roadmap_brochure.pdf?search=search
- Cavoukian, Ann., El Emam, Khaled, *A Positive-Sum Paradigm in Action in the Health Sector* (Office of the Information and Privacy Commissioner, Ontario, Canada, March 2010), http://www.ipc.on.ca/images/Resources/positive-sum-khalid.pdf
- Alvarez, C. Richard., Cavoukian, Ann, *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities - Win/ Win* (Office of the Information and Privacy Commissioner, Ontario, Canada, March 2012). www.ipc.on.ca/images/Resources/2012-03-02-PbD-EHR.pdf
- Cavoukian, Ann., Hoffman, David., & Killen, Scott. *Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design* (Office of the Information and Privacy Commissioner, Ontario, Canada, November 2009), http://www.ipc.on.ca/images/Resources/pbd-remotehomehealthcarew_Intel_GE.pdf
- Cavoukian, Ann., Mihailidis, Alex., Boger, Jennifer., *Sensors and In-Home Collection of Health Data: A Privacy by Design Approach* (Office of the Information and Privacy Commissioner, Ontario, Canada, August 2010), http://www.ipc.on.ca/images/Resources/pbd-sensor-in-home.pdf
- Office of the Information & Privacy Commissioner of Ontario, *Innovative Wireless Home Care Services: Protecting Privacy and Personal Health Information* (Office of the Information and Privacy Commissioner, Ontario, Canada, April 2009), http://www.ipc.on.ca/images/Resources/wirelesshomecare.pdf

- Cavoukian, Ann. *Abandon Zero-Sum, Simplistic either/or Solutions - Positive-sum is Paramount: Achieving Public Safety and Privacy Concept* (Office of the Information and Privacy Commissioner, Ontario, Canada, November 2012) http://www.ipc.on.ca/images/Resources/pbd-ctc.pdf

5. End-to-End Security – ***Full Lifecycle Protection***

- Cavoukian, Ann, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report MC07-68*, (Office of the Information and Privacy Commissioner, Ontario, Canada, March 2008), http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf
- "Fact Sheet 16: Health-Care Requirement for Strong Encryption" (Office of the Information and Privacy Commissioner, Ontario, Canada, July 2010), http://www.ipc.on.ca/images/Resources/fact-16-e.pdf
- Curtis, Jeff.,& Jolly, Nandini., *Encryption by Default and Circle of Trust*, (Office of the Information and Privacy Commissioner, Ontario, Canada, November 2012)
- *Video Surveillance Cameras: An Innovative Privacy-Enhancing Approach*, (Office of the Information and Privacy Commissioner, Ontario, Canada, March 2008)
- Cavoukian, Ann., & Johnson, Robert. *Get rid of it Securely to keep it private: Best practices for the secure destruction of personal health information* (Office of the Information and Privacy Commissioner, Ontario, Canada, October 2009), http://www.ipc.on.ca/images/Resources/naid.pdf
- Cavoukian, Ann, *If You Want To Protect Your Privacy, Secure Your Gmail*, (Office of the Information and Privacy Commissioner, Ontario, Canada, July 2009), http://bit.ly/COvz3
- Cavoukian, Ann., Zeng, Ke, *Modelling Cloud Computing Architecture Without Compromising Privacy: a Privacy by Design Approach* (Office of the Information and Privacy Commissioner, Ontario, Canada, May 2010), http://bit.ly/aVjFBC

6. ***Visibility*** and ***Transparency*** – Keep it ***Open***

- Cavoukian, Ann. *Guidelines for the Use of Video Surveillance Cameras in Public Places* (Office of the Information and Privacy Commissioner, Ontario, Canada, September 2007), http://www.ipc.on.ca/images/Resources/video-e.pdf
- Cavoukian, Ann. *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*, (Office of the Information and Privacy Commissioner, Ontario, Canada, June 2006), http://www.ipc.on.ca/images/Resources/rfid-guides&tips.pdf
- Cavoukian, Ann., Garcia, Victor. *RFID and Privacy – Guidance for Health-Care Providers*, (Office of the Information & Privacy Commissioner, Ontario, Canada, January 2008), http://www.ipc.on.ca/images/Resources/rfid-HealthCare.pdf

- *Short Notice to the Public under the Personal Health Information Protection Act: Your Health Information and Your Privacy in Our Office* (Office of the Information and Privacy Commissioner, Ontario, Canada, June 2005) http://www.ipc.on.ca/index.asp?navid=46&fid1=257&fid2=2

- *Short Notice to the Public under the Personal Health Information Protection Act: Your Health Information and Your Privacy in Our Hospital* (Office of the Information and Privacy Commissioner, Ontario, Canada, June 2005) http://www.ipc.on.ca/index.asp?navid=46&fid1=259&fid2=2

- *Short Notice to the Public under the Personal Health Information Protection Act: Your Health Information and Your Privacy in Our Facility* (Office of the Information and Privacy Commissioner, Ontario, Canada, June 2005) http://www.ipc.on.ca/index.asp?navid=46&fid1=261&fid2=2

7. ***Respect*** for the User – Keep it ***User-Centric***

- Cavoukian, Ann. *Privacy and Government 2.0: The Implications of an Open World* (Office of the Information and Privacy Commissioner, Ontario, Canada, May 2009) http://www.ipc.on.ca/images/Resources/priv-gov-2.0.pdf

- Cavoukian, Ann., Weiss, B. Justin, *Privacy by Design and User Interfaces: Emerging Design Criteria - Keep it User-Centric* (Office of the Information and Privacy Commissioner, Ontario, Canada, June 2012), http://www.ipc.on.ca/images/Resources/pbd-user-interfaces_Yahoo.pdf

- Cavoukian, Ann. *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age* (Office of the Information and Privacy Commissioner, Ontario, Canada, October 2006), **http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf**

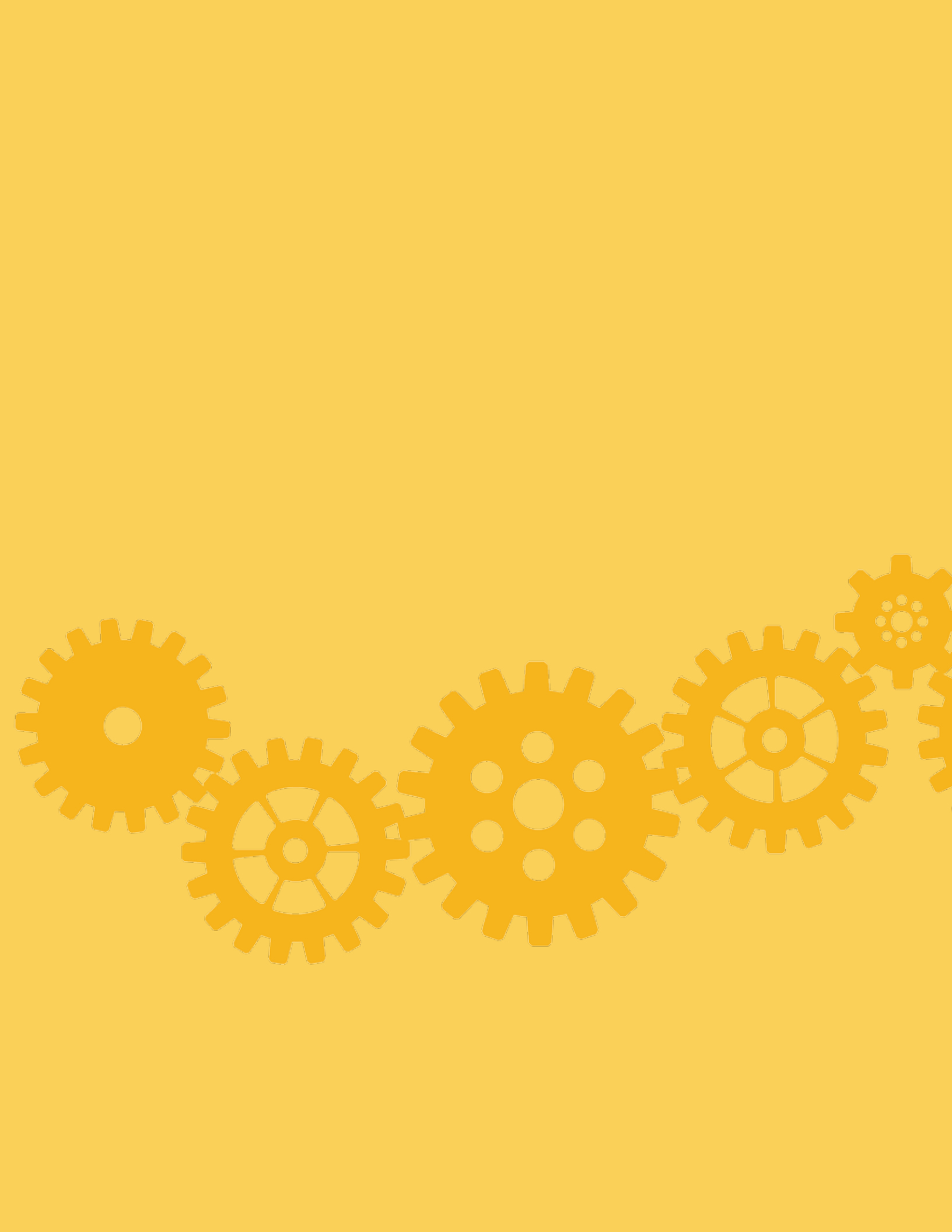
- Green, Shane., Galper, Josh., Reed, Drummond., Brandt, Liz., Mitchell, Alan., Cavoukian, Ann. *Privacy by Design and the Emerging Personal Data Ecosystem,* (Office of the Information and Privacy Commissioner, Ontario, Canada, October 2012) http://www.ipc.on.ca/images/Resources/pbd-pde.pdf

- Tomko, G. J., Borrett, D. S., Kwan, H. C., & Steffan, G. (2010). SmartData: Make the data "think" for itself. Identity in the Information Society, 3(2), 343-362

- to be published Cavoukian, Ann. *Privacy by Design: Leadership, Methods, and Results* Paper presented at the 5th International Conference on Computers, Privacy & Data Protection European Data Protection: Coming of Age, Brussels, Belgium.

- Cavoukian, A. (2012). *Privacy by Design*: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (pp. 170-208): IGI Global.

- Cavoukian, A. (2012). Strategies for Operationalizing Privacy by Default. *Privacy & Compliance Tijdschrift Voor De Praktijk* (03-04/2012 *Privacy by Design*), 17 - 20.



Ann Cavoukian, Ph.D.

Information and Privacy Commissioner, Ontario, Canada

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

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca
Telephone: 416-326-3333
Fax: 416-325-9195

December 2012