IDIS (2010) 3:247–251
DOI 10.1007/s12394-010-0062-y

Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D

Ann Cavoukian

Received: 10 March 2010 / Accepted: 5 May 2010 / Published online: 18 May 2010

Keywords Privacy by design · Privacy-enhancing technologies · Positive-sum

In November, 2009, a prominent group of privacy professionals, business leaders, information technology specialists, and academics gathered in Madrid to discuss how the next set of threats to privacy could best be addressed.

The event, *Privacy by Design: The Definitive Workshop*, was co-hosted by my office and that of the Israeli Law, Information and Technology Authority. It marked the latest step in a journey that I began in the 1990's, when I first focused on enlisting the support of technologies that could enhance privacy. Back then, privacy protection relied primarily upon legislation and regulatory frameworks—in an effort to offer remedies for data breaches, after they had occurred. As information technology became increasingly interconnected and the volume of personal information collected began to explode, it became clear that a new way of thinking about privacy was needed.

Privacy-Enhancing Technologies (PETs) paved the way for that new direction, highlighting how the universal principles of fair information practices could be reflected in information and communication technologies to achieve strong privacy protection. While the idea seemed radical at the time,[1] it has been very gratifying over the past 15 years to see it come into widespread usage as part of the vocabulary of both privacy and information technology professionals.

But the privacy landscape continues to evolve. So, like the technologies that shape and reshape the world in which we live, the privacy conversation must

[1] When Commissioner Cavoukian and John Borking (representing Commissioner Peter Hustinx) of the Dutch Data Protection Authority first presented their joint paper in 1995, *Privacy-Enhancing Technologies: The Path to Anonymity*, in Brussels, it was met with silence by the Commissioners in attendance. It was a further three years before the message strongly took hold and the concept gained global momentum.

A. Cavoukian (✉)
Information & Privacy Commissioner, Ontario, Canada
e-mail: commissioner@ipc.on.ca

continually renew and sharpen its focus. These days, the stakes are high; perhaps higher than they've ever been before. Privacy is coming under increasing pressure from many different forces including online social networks, an explosion in social media, governments and businesses providing services that are highly individualized and information-dependent.

The importance of privacy cannot be overstated. Our essential freedoms and liberty rest upon it. Indeed, history has demonstrated that privacy is the first thread to unravel as a free and democratic state morphs into a totalitarian state. As long as we value liberty—we must also value privacy.

Over the years, a zero-sum paradigm has prevailed, in which one value, such as privacy, competes with another value, such as security, in a zero-sum "win-lose" equation: The thinking goes along the lines of—in order to have adequate security and protect ourselves against the threat of terrorism, we must forfeit our privacy. This notion, however, is based on completely flawed logic and a false dichotomy—that privacy and security must be considered mutually opposing, which is simply not true.

Privacy *can* and *must* co-exist alongside other critical requirements: security, functionality, operational efficiency, organizational control, business processes, and usability in a "positive-sum", or doubly enabling "win-win" equation.

How we get there is through *Privacy by Design*. Where PETs focused us on the positive potential of technology, *Privacy by Design* prescribes that we build privacy directly into the design and operation, not only of technology, but also of operational systems, work processes, management structures, physical spaces and networked infrastructure. In this sense, *Privacy by Design* is the next step in the evolution of the privacy dialogue.

Engaging in that conversation means engaging with technology, in all the myriad directions it is heading. Each evolution, each new design, each new implementation, is an opportunity to carry our core values well into the future, rather than allowing the future to fade them away.

Twenty years ago, privacy advocates were focused on how to address the privacy implications of technologies that automated functions that had previously been paper-based. Now, mapping the direction of technological change, we can see a mounting interest in, and emphasis on, dense internetworking, large-scale data sharing, and new kinds of relationships between organizations. Firms are moving from multinational to global in nature, and the concept of an enterprise is being replaced by that of an ecosystem.

In the online realm, concepts such as cloud computing, in which organizations share processing resources (and possibly data) to co-ordinate business processes and operations, are taking hold, creating new opportunities for collaboration. This marks a significant change from earlier enterprise-based models that were predicated on individuals interacting with (and providing information to) companies with which they have an established (and often, trusted) business relationship. In the emerging model, information may be shared within and across enterprises and value chains.

Certainly, these developments are of great interest to those of us concerned with privacy and who seek to ensure that privacy remains protected, as these interactions evolve. Thankfully, this also piques the interest of the very enterprises engaged in ushering in this new future. Why? Because cloud computing, inter-networking, and large-scale data sharing require a simple but powerful, and often elusive feature in order to succeed: trust.

In the past, the development of the Internet and the possibility of electronic commerce created demand for mechanisms to enable people and organizations to trust one another. Now, faced with increasingly diffused and complex relationships between consumers and the organizations they do business with, as well as new forms of interaction between organizations working together in federated models, the need for trust is greater than ever before. And yet, it is becoming more elusive and harder to earn. Responsible information management practices, including paying close attention to the protection of personal information, form an important part of building and maintaining successful relationships in this new world.

For years I have argued that privacy is good for business (as evidenced by the title of my book: *The Privacy Payoff*), and that only becomes more true as time goes by. The business case for privacy focuses on gaining and maintaining customer trust, breeding loyalty, and generating repeat business. The value proposition typically reflects the following:

1. Consumer trust drives successful customer relationship management (CRM) and lifetime value… in other words, business revenues;
2. Broken trust will result in a loss of market share and revenue, translating into lower stock value;
3. Consumer trust hinges critically on the strength and credibility of an organization's data privacy policies and practices.

In a marketplace where organizations are banding together to offer suites of goods and services, trust is clearly essential. Indeed, the success of this business model is heavily dependent on the ability of members to demonstrate their trusted privacy practices across the federation.

Of course, trust is not simply an end-user issue. Companies that have done the work to gain the trust of their customers cannot risk losing it as a result of another organization's poor business practices. So the internal strength and growth of a federation is dependent on the extent to which members of the federation can trust that established policies, procedures and technological rules are followed and respected by all involved. Internal growth and strength can translate into powerful differentiation in the marketplace and lasting competitive advantage; as noted earlier, what I call the "Privacy Payoff."

Just as regulatory approaches proved to be necessary but not sufficient 20 years ago, we can see now that Privacy-Enhancing Technologies are necessary but not sufficient to protect privacy and provide a foundation of trust well into the future. That is why the concept of *Privacy by Design* extends to a trilogy of encompassing applications: 1) IT systems, 2) accountable business practices, and 3) physical design and networked infrastructure.

Implementing *Privacy by Design* (PbD) means focusing on, and living up to, the following 7 Foundational Principles, which form the essence of PbD:

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

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

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

   We can all be certain of one thing—the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy 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 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, or doubly enabling "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. It avoids the pretense of false dichotomies, such as privacy ***vs.*** security, demonstrating that it ***is*** possible to have both.
5. End-to-End Lifecycle Protection

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

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

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

These are precisely the principles that informed the debate and discussions that took place at the event *Privacy by Design: The Definitive Workshop* in November, 2009. What became clear from the day's proceedings was that *Privacy by Design* was a concept whose time has come. Tremendously adaptable, its principles are relevant whether we are talking about electricity grids going smart, the future of the Internet, SmartData, biometrics, home health care, or any other area.

Indeed, you will find represented in this selection of papers from the day's proceedings a very wide variety of disciplines, perspectives, and industries. And while several of the papers focus on technology, you'll also find discussions of how *Privacy by Design* can be used to approach operational and management issues. This is, in fact, one of the key benefits of the evolution in thinking from Privacy-

Enhancing Technologies to *Privacy by Design*: it allows us to consider technology, business processes, management functions and other organizational issues in a comprehensive manner and to embed privacy at every layer.

By doing so, I believe that *Privacy by Design* will assist in creating a particular culture of privacy which I have been advocating for many years. This culture of privacy is what emerges when organizations approach privacy not as a compliance issue, but as a business issue. It is what takes hold when the leadership of an organization comes to see that the implementation of positive privacy controls creates—rather than constrains—business opportunities. In short, it is a culture of "win-win" or positive-sum.

Of course, as a Commissioner tasked with overseeing privacy laws, I do not suggest that *Privacy by Design* should be applied in a vacuum. It is a critical part—but only a part—of a suite of privacy protections that brings together regulatory instruments, consumer awareness and education, accountability and transparency, audit and control, and market forces.

The selection of papers in this special issue of the IDIS Journal captures the energy and dynamism of the Madrid workshop. There is tremendous excitement about how *Privacy by Design* can enable all of us to approach technology, systems design, operations, and management issues in ways that maximize privacy, while delivering on business objectives. It is very exciting in the way, if I may be so bold, that victory often is. And doubly so, in my view, because understanding privacy through the lens of a positive-sum paradigm allows everyone to share in that victory.