Privacy by Design

ANN CAVOUKIAN

In the 1990s, it became clear to me as the Information and Privacy Commissioner of Ontario, Canada, that to safeguard privacy – an essential and foundational requirement of our rights and freedoms – legislation and regulation would no longer be sufficient. With the increasing complexity and interconnectedness of information technologies, in my view nothing short of building privacy right into system design could suffice. That is why I developed Privacy by Design (PbD), the framework to proactively embed privacy directly into information technology, business practices, physical design, and networked infrastructures – making it the default.

Privacy by Design is the international standard[1] for assuring privacy in the information era.

Commitment to PbD has grown rapidly with the support of my Canadian federal and provincial counterparts, data protection and privacy commissioners from around the world, as well as a growing legion of PbD Ambassadors. In fact, in October 2010, Privacy by Design was unanimously adopted as an international privacy standard at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem. Data protection authorities from around the world pledged to advance the 7 Foundational Principles [1] of PbD in their respective jurisdictions. Since then, the U.S. Federal Trade Commission recommended the use of PbD in its proposed privacy framework for commercial entities, and the European Union is integrating PbD into revised privacy regulations.

More organizations than ever in the public and private sectors have now operationalized the principles of PbD, embedding them into the way they think, do business, design products, and deliver services. Here in my jurisdiction of Ontario, Canada's most populous province, one of the most recent successful applications of PbD to real world business operations was a partnership between my office, the University of Toronto, and the Ontario Lottery Group (OLG). Our paper, "Privacy-protective facial recognition: Biometric encryption proof of concept" [2] outlines the 2011 rollout of a face recognition system for casinos and gaming facilities capable of identifying 15 000 individual participants in a voluntary self-exclusion program for problem gamblers, while protecting their privacy and that of the other hundreds of thousands of patrons. This first-of-its-kind technology, coupled with updates to the photographic elements, achieves a best-case result of 91% identification.

Yet another successful PbD innovation is our ongoing work with the Smart Grid and Smart Meters. In 2009, I brought forward the point that privacy in the Smart Grid was a "sleeper issue" that needed to be addressed as one of the critical success factors to implementing the Smart Grid. We approached this by issuing a number of publications, such as "Operationalizing Privacy by Design: The Ontario Smart Grid Case Study" [3]. Moreover, we have also partnered with San Diego Gas & Electric (a division of Sempra Energy, a Fortune 500 company) to co-author "Applying Privacy by Design best practices to SDG&E's Smart Pricing Program"

[1] This is the result of a landmark resolution passed by international Data Protection and Privacy Commissioners at their annual conference in Jerusalem in 2010: http://www.ipc.on.ca/images/Resources/2010-10-29-Resolution-e_1.pdf.

Digital Object Identifier 10.1109/MTS.2012.2225459
Date of publication: 19 December 2012

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

[4], and published a further paper entitled "Smart meters in Europe: Privacy by Design at its best" [5].

As we have demonstrated, the task for privacy-aware engineers and systems architects is to translate the PbD conceptual framework into a set of specific, and operationally feasible, tools. When applied by designers and project managers, these tools will ensure that business requirements, engineering specifications, development methodologies, security controls and best practices will be developed or applied according to each domain or project scope – with privacy as the context.

This is why I declared 2011 as the "Year of the Engineer," believing that I needed to reach out beyond regulators and policy-makers, to those who actually design and build the systems and infrastructure. I spoke to mobile app developers, research labs, tech start-ups, multinationals, industry consortia and standards groups, information and security architects, and engineers at companies such as Adobe, Google, and RIM, who all got the message that privacy is critical to their operations. Privacy is a team sport; it requires cooperation among all stakeholders – whether inside one organization or across an entire industry or sector – to be truly effective.

To provide further guidance, in October we published a how-to paper on operationalizing Privacy by Design, which will augment our current papers addressing how to implement PbD in specific areas.

The task for privacy-aware engineers and systems architects is to translate the Privacy by Design conceptual framework into a set of specific, and operationally feasible, tools.

I'd also like to clear up a common misconception that privacy somehow stifles innovation. Not true! In fact, protecting privacy demands the highest level of innovation. This year I am calling on all innovators and inventors to enlist technology to help protect our privacy well into the future, in what I am calling the "Year of the Innovator." In the midst of today's unprecedented explosion of information technology and the privacy challenges that come with it, we will need innovators to come up with the solutions we need to protect privacy.

I have also begun to focus on game-changing solutions such as SmartData. SmartData consists of Internet-based autonomous agents that act as a data subject's online surrogate, securely storing one's personal information, and intelligently disclosing it based upon the context of the data request, and in accordance with the user's instructions. This approach is based on the idea that natural evolution remains the best roadmap available for building artificial agents that possess the property of contextual processing. In effect, we are attempting to shrink the security perimeter from a mass of collective personal data stored in a database, down to a single individual's sphere of personal data. One's personal data will then be wrapped in a "cloak of intelligence" such that this entity, SmartData, becomes the individual's virtual proxy in cyberspace, controlling the release of their data. SmartData proactively builds privacy and security in, right from the outset, so that nothing is treated as an afterthought. It embodies a foundation of control and trust within the technology itself, incorporating the principles of purpose specification, personal consent, security, and use limitation.

SmartData follows in the spirit of PbD, or what I now call PbD 2.0. It endorses the use of technology (artificial intelligence) to protect privacy and our civil liberties. SmartData can empower our personal data with the ability to protect itself in a manner that is perceptive to the needs of the data subject (the individual), while enabling multiple functionalities that make authorized requests for data.

As a privacy professional, I believe that the widespread accommodation of privacy as a core system requirement is poised to become one of the key trends of our time. We can, and must, have both privacy and security, privacy and business, privacy and other necessary functionalities. We only need to embrace a positive-sum paradigm. We must replace the "vs." with "and," allowing for a win-win solution – for us, and for our free and open society.

References

[1] A. Cavoukian, "PbD origin and evolution," *Privacy by Design,* 2012; http://privacybydesign.ca/publications/pbd-origin-and-evolution/page/2/.

[2] "Privacy-protective facial recognition: biometric encryption proof of concept," Information and Privacy Commissioner of Ontario, 2012; http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1000.

[3] "Operationalizing *Privacy by Design*: The Ontario Smart Grid Case Study," Information and Privacy Commissioner of Ontario, 2012; http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1037.

[4] A. Cavoukian and C. Winn, "Applying Privacy by Design Best Practices to SDG&E's Smart Pricing Program," www.privacybydesign.com, Mar. 2012; http://www.ipc.on.ca/images/Resources/pbd-sdge.pdf.

[5] A. Cavoukian, "Smart meters in Europe: Privacy by Design at its best," www.privacybydesign.com, Apr. 2012; http://www.ipc.on.ca/images/Resources/pbd-smartmeters-europe.pdf.