Theme Article: Special Section on Privacy and Security by Design

Understanding How to Implement Privacy by Design, One Step at a Time

Ann Cavoukian
Global Privacy and Security by Design Centre

***Abstract*—While widely accepted as a game changer for protecting privacy, Privacy by Design (PbD) has also developed a reputation for being challenging to implement for businesses. The reality is much different. PbD was intended to form the foundation of how to proactively embed privacy into the design of products and services. This is why the 7 principles of PbD are called Foundational Principles. They can be actualized and customized in many different ways, depending on the particular requirements of an organization. This article will present a simplified discussion of practically implementing PbD and how PbD can enhance corporate interests, while offering the strongest privacy and data protection to achieve multiple goals. It's a clear: win/win!**

While widely accepted as a game changer for protecting privacy, privacy by design (PbD) has also developed a reputation for being challenging to implement for businesses. The reality is much different. PbD was intended to form the foundation of how to proactively embed privacy into the design of one's operations, broadly speaking. This is why the seven principles of PbD are called Foundational Principles—to form the foundation of your privacy operations. PbD can be actualized and customized in many different ways, depending on the particular requirements of the organization. In fact, PbD has been successfully adopted by businesses across a variety of industries and markets, including telecommunications and authentication services. These businesses, which all operate in disparate

Digital Object Identifier 10.1109/MCE.2019.2953739
Date of current version 7 February 2020.

Published by the IEEE Consumer Electronics Society

sectors of the economy, have one thing in common: they have chosen to put privacy at the center of their product and service developments, and have found that it gave them a competitive edge. Learning from these businesses about the keys to their successful PbD implementation can help organizations across industries understand how PbD can enhance their corporate interests, while offering the strongest privacy and data protection to achieve multiple goals. It is a clear win/win!

PbD has been widely acclaimed for its benefits to both businesses and consumers; it offers a road map to build much-needed privacy protections into new applications, tools, and services, so that developers may begin their design process by thinking about privacy. As seen too frequently in the media, recent news stories show us the frequency and dire consequences of those who overlook the importance of privacy, as incidents of data breaches and data mishandling continue to rise. PbD offers a way for businesses to avoid these problems by not simply thinking about privacy as an add-on after new products and services have already been designed, developed, or launched, but rather to lead with, and factor privacy into, the process of creating new offerings.

Moreover, PbD is becoming the norm for international privacy compliance. Europe's General Data Protection Regulation (GDPR) incorporates "data protection by design" and "data protection by default" (the second Foundational Principle of PbD), into its requirements for organizations under Article 25. These GDPR legal requirements build on the Foundational Principles of PbD. The European Data Protection Commissioner defines PbD as: "The broad concept of technological measures for ensuring privacy as it has developed in an international debate over the last few decades," while the term "data protection by design" refers to the focused requirements in Article 25, which represent a direct proactive implementation and application of the more visionary and ethical dimensions of PbD.

As media attention continues to focus on incidents of privacy misdeeds, the interest and use of PbD are further expanding. Soon, a new International Standards Organization standard for PbD (currently before the ISO project committee ISO/PC 317, and distinct from ISO/IEC 27701, which includes PbD within broader privacy and security requirements) will become a best practice for businesses around the world interested in building privacy protections directly into their products and services. Likewise, business models building around PbD with consulting firms are becoming affiliated with research centers and certification groups in order to enhance the knowledge of PbD within organizations. However, a hurdle for some organizations to fully implement PbD into business practices remains the challenge of building, what is at times characterized as a complex set of principles into a practical set of business standards applicable to day-to-day business functions. And yet the foundational principles of PbD were intended to be proscriptive, pointing the way forward to being applied to a particular company's operations.

Many businesses have taken up the cause of implementation, and have witnessed the tremendous success that PbD can bring to a business. Businesses that have embraced the possibility of PbD for their new initiatives make it clear that simple steps go a long way to making PbD a game changer for businesses that can greatly enhance the customer trust with organizations. One early adopter of PbD in Canada was TELUS Communications, Inc. TELUS successfully embraced PbD principles, not simply in their corporate policies, but by customizing the seven PbD principles into practical business guidance, which is then reinforced through training and project-specific implementation and partnerships.

As referenced above, PbD thinking is powered by its seven Foundational Principles:

1) proactive not reactive, which focuses on prevention;
2) privacy as the default setting;
3) privacy embedded into design;
4) full functionality (not zero-sum!);
5) end-to-end security;
6) visibility and transparency; and
7) respect for user privacy.

From these essential principles, large consulting houses such as Deloitte and KPMG have developed criteria and controls that add the functional considerations for the implementation of these principles into successful business practices.

For some companies, these principles have been transformed into specifications and recommendations that can be used by those across the company, for a variety of projects. These specifications provide additional guidance to each of the seven principles by outlining what the "to do" item should be for anyone undertaking a project; these are practical suggestions for employees that are easily and broadly applied to new initiatives. Most important, organizations who embrace PbD should consider how the seven foundational principles can become contextualized for the unique considerations of their organization, thereby allowing PbD to become real and tangible for employees.

For many companies, the successful implementation of PbD starts with expanding awareness of the seven principles, through training and education programs. For example, "Privacy as the Default" is a game changer, shifting the consent model away from negative consent to positive consent: "opt-in" not "opt-out." At TELUS Communications, the company has focused on leveraging ongoing training to encourage longer term engagement with the program. Using training as an entry point for team engagement has also meant that as new privacy challenges arise, teams outside of the compliance realm seek advice and counsel from the privacy team about new challenges and updates to tools already in existence, thereby eliminating the disconnected "silo" problem.

"Our Data & Trust Office team proactively works to identify key senior stakeholders at TELUS who have teams that would benefit from training," said Pamela Snively, Chief Data & Trust Officer at TELUS. "Working with those leaders we actively engage teams on PbD, the seven principles and key considerations for the teams to think about when undertaking the types of projects they work on. Most importantly, we ensure that teams know where to come for assistance within my team. It is really about building a collaborative culture to support Privacy by Design at all stages of development."

Perhaps the greatest challenges to a privacy regime are those unique projects that require additional collaboration between the Privacy Office and project teams. With new and evolving technologies come enhanced privacy risks that PbD is well suited to address. However, the unique challenges of these projects often require hands-on collaboration between various teams. For TELUS, projects involving augmented intelligence, Internet of Things, and mobility are especially important to handle with care, to ensure that PbD is fully realized by the teams in order to mitigate any privacy risks. "We have realized the benefits of working with the Data & Trust (Privacy) Office. We have embodied PbD into our TELUS Insights products and services, and believe that part of putting our Customer First is putting their privacy first," said Michael Cihra, VP of Internet of Things and Insights at TELUS.

Another area where TELUS enhances privacy and security for consumers is by incorporating PbD into its SmartHome Security services. SmartHome offers customers real-time home monitoring capabilities for security, as well as fire, floods, and carbon monoxide alarm notifications. Customers are able to see notifications in their home, as well as through mobile device connections. At TELUS, a member of the Data & Trust Office, called a Privacy Partner, is embedded within the SmartHome team, providing support for their privacy efforts during day-to-day operations, including participating in strategic planning, and design thinking workshops. "In this model the Data & Trust Office is not viewed as a distinct business unit or department that is engaged on an as-needed basis, but is engaged as a partner that enables initiatives to launch seamlessly," said Blair Miller, VP of Content Solutions at TELUS. Throughout, the privacy partner ensures that PbD is not an afterthought in the development of services, but is at the forefront of the team's thinking when making plans. This is a PbD dream come true, working proactively to prevent the privacy harms from ever arising in the first place!

Through these series of measures such as contextualizing the seven PbD principles to make them task-oriented and specific to the needs of the organization, developing training that is provided proactively and working collaboratively with teams on uniquely challenging data use projects, PbD can be successfully implemented in organizations across industries, giving employees the knowledge and tools they need to turn its principles into day-to-day solid actions. Ensuring

that PbD principles are adapted to the needs of an organization helps us to drive usability and implementation, in order to drive greater adoption and stronger privacy protections.

There are numerous other companies who follow PbD and have become certified for PbD. The benefits of building trusted business relationships with customers by offering them enhanced privacy, while enabling business interests to grow, lead to a discernible competitive advantage! Examples of this are Intel and GE, who used PbD to address remote home health care technologies. They identified which privacy considerations needed to be addressed and designed them directly into the system in a positive-sum manner. This enables strong protection of personal data while maintaining the functionality and health benefits of the remote technologies being used. For instance, the elderly often wish to remain in their homes, even when living there alone, but they may require some additional help from time to time. Intel created sensors that could be strategically placed in the homes of seniors to offer them much-needed assistance, when required. If someone got up in the middle of the night to use the rest room, but did not return to bed within a predetermined period of time, the sensor attached to their bed would release a signal for help. But, the wireless communication released by the sensor would be strongly encrypted (to prevent any unauthorized access), and would only be received by the three individuals who were preauthorized to provide much-needed assistance: so what is ultimately delivered by the service is privacy protection and necessary healthcare.

IBM has also taken PbD "from policy to practice." IBM put a strategic, proactive focus on privacy, enabling process improvements that were demonstrably linked to a reduction in operational costs, which supported IBM's business strategy of always providing strong data protection to their customers, through PbD.

One of the essentials we should never overlook is the need for strong security, from end-to-end, with full lifecycle protection. While the term privacy subsumes a much broader set of protections than security alone, in this day and age of daily cybersecurity attacks, if you do not have a strong foundation of security, across the entire enterprise, you would not have any privacy, full stop! Security is essential to privacy—they go hand-in-hand. This is one of the reasons I decided to call my new company the "Global Privacy & Security by Design Centre," in an effort to emphasize the need for both privacy and security, working in unison, hand-in-hand, not as opposing forces (as I already mentioned, it is definitely time to get rid of zero-sum mindsets).

There is also a growing public acceptance of technology solutions, which give consumers more security, privacy, and greater control over their personal data. One example is a new company called My2Tec Inc., which is developing a technology to store a user's personal data securely, in encrypted form, within their own secure cloud space, allowing the user to query their data via their own personal intelligent agent. My2Tec would also enable people to have their personal information used for privacy-preserving and permissioned data analytics, should they wish to do so. Can you imagine a world where we could each have our own personal digital assistant, to do our bidding, in a totally privacy and security preserving way? My2Tec would ensure that both privacy and security are embedded throughout the entire process, by Design! Here is to a future where privacy and security are seamlessly embedded and baked into the code.

From the examples provided by TELUS, Intel, GE, IBM, and My2Tec, it is apparent that implementing PbD into regular business practices is not actually the challenge that some may assume, but, instead, a highly practical and strategic decision to put privacy at the forefront of a company's goals. The difference between those who choose to implement PbD and those who do not is often simply a difference in priority—who is considering the needs of their customers and valuing their privacy in business practice? While some legwork may be needed to translate the seven Foundational Principles into actionable training and specifications, the value to a company is immense in terms of the positive effect that this has on its customers. At this time of steadily increasing trust deficits, PbD is a smart strategic value proposition for any company wishing to lead through smart privacy and data protection, thereby building consumer trust, and in turn, gaining a competitive advantage—win/win!

Ann Cavoukian is one of the world's leading privacy experts. She received the Ph.D. degree in psychology, specialized in criminology and law from University of Toronto. She is presently the Executive Director of the Global Privacy and Security by Design Centre, and is also a Senior Fellow of the Ted Rogers Leadership Centre at Ryerson University. She was the Information and Privacy Commissioner of Ontario, Canada, from 1997–2014. She served an unprecedented three terms as a Commissioner. Contact her at ann.cavoukian@gpsbydesigncentre.com.