Privacy by Design: From Policy to Practice

September 2011
Acknowledgements

The Information & Privacy Commissioner of Ontario, Canada wishes to acknowledge and thank the IBM Corporation for sharing this valuable case study of how an organization – even one of the scale and global reach of IBM – can implement Privacy by Design. Particular thanks are due to Harriet Pearson, VP Security Counsel & Chief Privacy Officer; Yim Chan, Global Privacy & Data Protection Executive & IBM Canada Chief Privacy Officer; and Howard Young, Privacy Program Manager.
Table of Contents

Foreword ......................................................................................................... 1

Introduction .................................................................................................... 3

Moving from Policy to Practice ....................................................................... 3

Privacy Self-Assessment Program and Tool ..................................................... 4

Privacy Education and Awareness Training .................................................... 7

Data Incident Management ............................................................................. 8

Lessons Learned .............................................................................................. 10

  Privacy Self-Assessments ............................................................................. 10
  Data Incident Response .............................................................................. 10
  Privacy Education and Awareness Training ................................................. 10
  Overall ....................................................................................................... 11

Key Benefits ................................................................................................... 11

Summary ......................................................................................................... 12
Foreword

Victor Hugo wasn’t thinking about Privacy by Design (PbD) when he wrote, “An invasion of armies can be resisted, but not an idea whose time has come.” Nonetheless, it nicely characterizes the steady growth in adoption of the concept. Frequently referenced since its inception, Privacy by Design has become a popular theme within the international privacy community over the past few years.

Privacy leaders from around the world, including Peter Hustinx – European Data Protection Supervisor¹; Viviane Reding – Vice President, Justice, Fundamental Rights and Citizenship, European Commission²; and, John Leibowitz – Chairman of the US Federal Trade Commission³, have endorsed the importance of PbD. At the 32nd Annual International Conference of Data Protection and Privacy Commissioners, I proposed a Privacy by Design Resolution⁴ that was unanimously passed and adopted. Considered a “landmark resolution,” it recognized Privacy by Design as an “essential component of fundamental privacy protection.”

Privacy by Design was born in the mid-90’s, when I realized that increasingly interconnected technologies would enable seemingly boundless collections of personal information. It became clear that we could no longer rely solely on compliance with legislation to ensure that privacy would be protected. Consequently, organizations needed to be encouraged to build privacy directly into technology, at the design phase, thereby ensuring the existence of privacy, right from the outset.

Although PbD’s roots lie in technology, over time, its application has been broadened to encompass accountable business processes and the design of physical spaces and networked infrastructure.

Privacy by Design is based on The 7 Foundational Principles⁵, which both affirm the Fair Information Practices and extend them, seeking the highest global standard possible. The principles are as follows:

1. **Proactive** not Reactive; **Preventative** not Remedial
2. Privacy as the **Default Setting**
3. Privacy **Embedded** into Design
4. Full Functionality – **Positive-Sum**, not Zero-Sum
5. End-to-End Security – **Full Lifecycle Protection**
6. **Visibility** and **Transparency** – Keep it Open
7. **Respect** for User Privacy – Keep it User-Centric

3. http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=dcc9e94bb69564313ae81e0f87976c4c&ContentType_id=14f995b9-dfa5-407a-9d35-56cc715a7ed&Group_id=b06e39af-e033-4c0a-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2010
Many organizations have begun to implement the principles of Privacy by Design. In this paper, we consider the case of the IBM Corporation, an early adopter. It is a transformative story of what can happen when PbD guides the architectural foundation of an enterprise’s operations. While it is not surprising that a complex, multi-national organization such as IBM would benefit from such a discipline, it is important to note that the lessons described are also applicable to organizations of any size.

For IBM, such a strategic focus on privacy has enabled process improvements that demonstrably link to reduced operational costs and documented compliance.

Achieving efficiencies is not the only, or even the most important, benefit of IBM’s PbD-based privacy practice, however. Beyond the foundational objectives at the heart of every organization’s privacy program, the team at Big Blue discovered that Privacy by Design enabled them to tackle more ambitious challenges – ones that directly supported the business strategy of the company. After all, an organization that aims to help its client build a “smarter planet” must do so from a position of trust and confidence, especially given the integral role that IBM plays in enabling the work and processing the data of many of the most important organizations in the world – from governments to consumer goods companies, to utilities, to health care organizations.

IBM’s journey from policy to practice is an important story. Along with the experiences of other organizations who have applied PbD, it serves to reinforce the fact that Privacy by Design is an idea whose time has truly come.

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

Privacy leaders know that even the best and most forward-looking privacy and data protection policies must be operationalized throughout an organization – by design – in order to be effective. International organizations face the additional challenge of meeting the requirements of multiple and disparate national and regional privacy laws.

The challenge is magnified at an enterprise such as IBM, whose business processes and operations span the globe, and whose workforce is geographically dispersed and culturally diverse. To meet such an enterprise-wide challenge, privacy and data protection policies must be embedded into the organizational fabric. At each level, lines of business and support functions (such as privacy and IT staff) need meaningful metrics to understand how the areas for which they are accountable are performing. Armed with these insights, they can then better manage how their part of the organization handles personal information.

IBM has found that a PbD-based approach is ideally suited to meet such requirements. One of PbD’s central tenets instructs that privacy be embedded directly into the design of accountable business processes and technologies. In striving to do so, IBM has made great strides in accomplishing other principles of PbD, such as: being proactive; meeting business objectives in a positive-sum manner; and generally creating a user-centric environment characterized by respect for privacy. The case study captured in this paper describes key components of IBM’s PbD program.

Moving from Policy to Practice

IBM’s commitment to privacy and data protection starts with an enterprise-wide privacy policy framework that was first adopted more than four decades ago, and which sets forth for all employees the all-important “tone from the top.” Of course, strong policies are necessary, but insufficient to address privacy risks and compliance obligations; implementation and strong oversight are required as well, especially at a large and diverse organization such as IBM.

To move from policy to practice, IBM’s strategy consists of three primary initiatives that form the pillars of the company’s PbD enterprise-level program:

1. Privacy Impact Assessments (PIA);
2. Privacy Education and Awareness Training; and
3. Data Incident Management.

Properly executed and implemented, Privacy Impact Assessments are a proactive way to identify and address business processes or IT applications that may benefit from enhanced safeguards to protect personal information.

---

6. IBM is a business employing over 400,000 employees, working in over 150 countries, and earning US $95.8 Billion in revenue in 2009.
Ongoing privacy education and awareness training gives all employees access to the information needed to recognize and properly handle personal information, on a day-to-day basis.

Data Incident Management is also necessary because an organization must be prepared for possible data breaches. If a data incident does occur, the organization must ensure that there are procedures in place to quickly manage the situation and to take proper steps to remediate and learn from the incident.

These three initiatives have evolved dynamically in the past decade as IBM’s privacy program has matured in response to changing internal and external demands and expectations. Starting as basic spreadsheets and presentation modules, the enabling tools in use today combine user-centric design; automated self-help diagnostics; and comprehensive capture and presentation of customized metrics. And, just as important, these tools have been embedded in the core processes of the company, on a worldwide basis.

Privacy Self-Assessment Program and Tool

For many organizations, PIAs are manual, time consuming and labour-intensive projects. It can take a great deal of time to generate the questions needed to identify privacy risk levels, to conduct interviews, and to review the answers collected. Typically, a subject matter expert must analyze the answers to determine the privacy risks, and then summarize the findings and recommendations. Some organizations have tried spreadsheet-based PIAs and have discovered that generating usable enterprise-level management reports is a daunting task. In practice, evaluating a single business process can require several weeks – or, at times, months – to determine its privacy risk.
PIAs are, nonetheless, a vital tool when practicing PbD, for when they are properly implemented they provide important oversight to ensure privacy compliance. To enable the proactive use of PIAs throughout its global enterprise, IBM developed, over five years ago, a web-based Privacy Self-Assessment Tool that may be applied to any business process or IT application within the company.

In designing its assessment methodology, IBM determined that individuals within each of their lines of business, rather than the Privacy Office, should be accountable for process and IT-application privacy compliance. There is also an important distinction between the following:

- **Business owner** – Person who is accountable for process compliance. They receive self-assessment results and agree to implement applicable actions.
- **Process owner** – Person who completes the privacy assessment on behalf of the business unit. This person may be the business owner or someone who is knowledgeable about the end-to-end process.

Regardless of who performs the assessment, because the business owner is understood ultimately to be responsible for compliance IBM has found that such self-assessments focus not only on the aspect of the process or associated IT application under consideration, but tend to also consider the implications for the end-to-end process: a key enabler of a PbD approach.

Once a business or process owner completes a self-assessment, their answers are analyzed by this Tool in real time. Immediately viewable – to the individual, as well as the corporate privacy office – is the privacy-related risk level associated with their process. The privacy risks identified are indicators of potential process and control gaps. The entire approach renders explicit, for the business owner, a set of potential opportunities to address privacy-related issues.

Business and process owners can complete the (roughly) 45 assessment questions in 30 minutes compared to the several weeks that may be required of a traditional PIA – an enormous time-saving. How is this achieved? IBM’s privacy, legal and technical teams worked closely together to design a tool and process that:

- Presents easy-to-understand questions (since business and process owners are not privacy experts);
- Uses an intuitive interface and logic flow that minimizes the need for training; and
- Provides **immediate** results upon completion of the tool, rather than weeks afterwards when the business or process owner would have moved on to other tasks and may have forgotten how they answered the questions.
Furthermore, institutional and regulatory knowledge and best practices are incorporated within IBM’s Privacy Self-Assessment Tool to make it easy for business and process owners to build a work plan to address any issues identified. A customized knowledge database can suggest over 100 unique actions that can be taken in response to the self-assessment’s findings. Once the action plan is finalized, it is tracked to completion.

The flow of the Privacy Self-Assessment Tool is illustrated in Figure 2. When a business or process owner signs on to the secure Intranet site, they are presented with a brief introduction to the Assessment Tool and simple instructions. Next, the questions in this Tool are answered. There are two types of questions:

- **Prologue Questions** address the types of personal information collected and where such information is used or managed. The answers to these questions then generate,

- **Assessment Questions** that are specific to the process being assessed and that take into account the countries involved, how the personal information is handled and who is processing it.

Once all the questions are answered, two graphical reports are immediately produced, displaying potential privacy risks. These interactive reports allow the business and process owners to click on the bar or pie charts to drill down for more details. If there are opportunities to enhance the privacy risk posture, the last – and critical – step is to build an action plan for closing them.

All self-assessment data and results are stored in a centrally managed database. Reporting tools provide metrics and scorecard measurements that summarize results at an enterprise, country and regional level for business unit executives and privacy focal points or champions. Reports also help IBM’s privacy team track the status of assessments falling within their area of support responsibility.

Since the entire process has been streamlined and in many cases automated, it enables privacy professionals to focus on adding substantive value rather than on managing the administrative tasks associated with individual assessments. For instance, email reminders are automatically triggered based on certain conditions (e.g., assessments that have not been started, or assessments with actions pending or past due).
Currently available globally for use throughout the company’s internal operations, “version 1.0” of IBM’s PIA tool and process originated in Canada as a way to enable streamlined compliance with the Personal Information and Protection of Electronic Documents Act. IBM’s privacy team has built on this foundation in a disciplined fashion by gradually expanding the regulatory information in this Tool’s knowledge base and then extending its availability to all geographies, including all the countries of the European Union. In this fashion, the privacy team has been able to establish consistent and informed privacy decision-making, well-informed by analysis and summary reports, throughout the enterprise.

Privacy Education and Awareness Training

In this digital world, understanding data privacy and how to manage sensitive information is something that employees need to know. While such awareness helps to achieve end-to-end security, an important PbD principle, it is also key to enabling a broader approach to privacy. Making employees aware of what is expected of them in this domain helps build a culture that values protecting personal information. Technology and security can only do so much; “privacy smart” employees are essential to effectively managing the organization’s personal information assets.

Everyone appreciates the importance of relevant and effective education. The challenge tackled by IBM was how best to organize the content and effectively deliver it. White papers, internal websites, pre-packaged presentations: these are all possible mechanisms for offering valuable information to one’s workforce, and are appropriately deployed in the right mix. What the IBM privacy team understood early on, however, is that while the content and messaging are important, one of the key considerations affecting retention is the format in which the educational content is delivered.

Therefore in building its customized Privacy Education and Awareness Tool, IBM focused on a technique to organize content based on “knowledge nuggets” or bite-size chunks of information that are easy for the student to digest. Each nugget is associated with a short take-away message.
The nuggets are organized into sections, each containing a case study illustrating a real situation that employees may face. Finally, there is a short, multiple choice quiz, where wrong answers yield pop-ups explaining the correct response. All of this is designed to increase information retention.

Every sign-in to the Privacy Education and Awareness Tool is logged and course progress is tracked electronically. Upon an employee’s successful completion of the course, a certificate is provided and course statistics are summarized for management use.

Importantly, two additional global, enterprise-wide awareness efforts complement and underpin these privacy-focused efforts. Each year, all IBM employees must complete a similar user-friendly course about, and certify their understanding of, the company’s “Business Conduct Guidelines.” Among other important topics, these Guidelines include privacy and information security. In addition, the entire IBM workforce receives information security-focused training. This workforce-wide training is supplemented by privacy and data security education and outreach within the company’s business and staff units.

Taken together, these ongoing efforts go a long way to raising awareness of and sensitivity to privacy and data protection throughout the enterprise.

**Data Incident Management**

It is increasingly important that organizations of all sizes be prepared to react to data security incidents. The causes of such incidents could range from malicious activities to inadvertent lapses in processes that handle personal data. Whenever and wherever they do happen, and for whatever reason, a disciplined and immediate response is important in order to address the situation in a manner that protects individuals, meets regulators’ expectations and ultimately preserves the reputation of the affected organization.

For a global enterprise, the response process must provide support and guidance with respect to, for example, the composition of the response team and the availability of expertise and resources to assist in the containment of a data breach. Policies regarding incident accountability need to be determined in advance to address situations that may involve multiple jurisdictions or business units.

Many companies currently use spreadsheets or similar tools to record information about data incidents. While this can be a convenient way to collect data about an incident, it has at least two drawbacks:

- Spreadsheets and other documents are likely stored on an individual’s personal computer, potentially increasing the difficulty of sharing information in a timely and secure manner; and
- The data collected in different parts of the world and by various business or staff units may be recorded inconsistently, making it difficult to cross reference or analyze trends and generate reports.
To overcome these issues, the IBM privacy team built a Web-based Data Incident Tool that standardizes the process by which the information is collected. In order to simplify the process, all data is stored in a common database. Access to this Tool and the data in it is governed via a series of user entitlement levels based on roles and responsibilities.

The process enabled by this Tool consists of four steps, starting with the opening of an incident. From start to finish, there is a minimum of 20 questions that need to be answered. Using an automated intelligent question logic flow, this Tool may prompt the asking of further questions in order to “drill down” into areas of particular importance.

In addition to collecting information about the incident, this Tool also guides the user to follow proper procedures. For example, in the case of a lost laptop, the user is prompted to also report the incident to the organization responsible for asset protection. This feature enables this Tool to be more than a simple repository of incident information.

After an incident is opened and based on answers to questions about location, type of incident, and potential risk, the Data Incident Tool identifies the designated expert who can support the incident response and then routes the relevant information to that individual. An email is automatically sent to an identified focal point to say that a data incident has been assigned to him or her. The incident “owner” can then access the Data Incident Tool and will rely on it for guidance through the steps needed to complete the investigation and bring the incident to closure.

The Data Incident Tool and associated processes offer a number of benefits:

- They standardize the response process and the information that needs to be collected across the enterprise;
- They serve as a repository for the investigation, follow-up and recovery activities associated with each incident, allowing authorized internal stakeholders to monitor and track the progress of the incident;
- Oversight and guidance are improved using reporting tools, which allow trend and root cause analysis, as well as scorecard metrics; and
• They improve incident response communication (both within the team and with stakeholders) through a consistent incident reporting process.

Lessons Learned

IBM’s goal of “turning privacy policy into practice” was facilitated by the development of self-help software tools and process. Through their deployment, several important lessons were learned.

Privacy Self-Assessments

Focus on actions to improve privacy, not on administrative tasks – Essentially proactive, the privacy self-assessment tool and process embodies and leverages the knowledge of IBM’s privacy experts and incorporates best practices. When opportunities to improve privacy and data protection are identified, this Tool suggests actions to take and enables IBM’s privacy team to focus on counseling and supporting the business -- instead of laboriously administering the assessment itself.

Start small, learn, and then expand – Starting a Privacy by Design program may be intimidating – regardless of the size of the organization. IBM’s privacy team started its PIA effort in a single country - Canada. They learned from that implementation, refined the program and then expanded elsewhere. A good practice is to select a manageable part of the enterprise and focus on optimizing a program there before scaling it to cover the entire enterprise.

Data Incident Response

Establish a consistent process – The Data Incident Tool is more about workflow and collaboration support than it is about data collection. Having this Tool identify an incident owner results in clear responsibility and accountability. Furthermore, the use of intelligent question logic flow drives higher-quality insights that enable rapid identification of the initial team needed to support incident response and minimize the repetition of unnecessary data collection or other tasks.

Adopt an architected approach to gathering incident information – Sharing information in a timely manner is critical for successful collaborations, which is precisely what is accomplished using this enterprise tool. Enabling consistent communication allows investigation team members to come together from different countries and different business units and functions. An architected approach also makes it possible to group similar incidents and look for root cause patterns across the enterprise.

Privacy Education and Awareness Training

Focus on students’ learning retention – Global organizations rely heavily on distance learning and self-study. While content is important, format and presentation are critical to learning and retention.

Embed privacy content where it matters – Rather than being satisfied with the production of a single comprehensive privacy module, IBM’s privacy team undertook a systematic campaign to identify partners throughout its organization with whom they could work to include privacy-
relevant materials into workforce communications and education. These partners have included Compliance, Information Technology/CIO and various business units. Doing so makes it more likely that privacy information will be seen by a larger number of employees at a time or place that is most relevant and beneficial.

Overall

**Partnerships and collaboration are key** – Regardless of the program (self-assessment, incident response or education), a *PbD* initiative will require close collaboration with a number of disciplines across the organization, such as IT and Legal.

**Disciplined data collection and presentation enables action and builds credibility** -- One of the most important features of IBM’s *PbD* program is the creation and sharing of fact-based and consistently presented metrics. Carefully designed and thoughtfully shared, these metrics enable the company’s privacy team to have focused and actionable discussions with a wide range of business and functional leaders.

**Key Benefits**

When IBM first started down the path of *PbD*-based enterprise privacy enablement, its goals were (and still are) to enable compliance and reduce privacy-related risk. While these goals continue to be important, other benefits and opportunities can and have been realized.

The Privacy Self-Assessment Tool is a good example. When IBM first introduced this Tool five years ago, it sought to reduce the risks associated with the handling of personal information. As a result of the thousands of completed assessments now on file, IBM has developed an inventory of the processes that collect and manage personal information. The resulting insights are significant. This rich inventory of processes and IT applications that manage personal data informs work to standardize procedures and processes that handle such data. Moreover, the inventory enables the privacy team and others to screen processes and probe whether they actually need to collect and use personal information in the first place: data minimization at work.

Other benefits of adopting a *Privacy by Design* approach include:

- **Efficiency through automation** – Wherever possible, IBM has automated these processes to realize efficiencies and more effectively deploy resources. Thus, global usage and transaction volumes of these tools and processes have increased without a commensurate increase in headcount or budget.

- **End-to-end focus to improve control and quality of the process** – IBM has looked at vertical processes that tie operational automation with oversight and governance procedures. The effect of this is a continuous monitoring and improvement cycle. Privacy focal points and business policy owners regularly receive reports that inform their governance process so that, if necessary, policies can be refined or new ones introduced. Oversight is also tied in and linked to business controls. The presence of this ecosystem supports the
implementation of IBM’s privacy policies throughout the enterprise, within a continuous improvement model.

Through global, documented and disciplined processes that have been implemented via automated self-help tools, IBM can now better:

• Identify business processes and applications that are collecting Personally Identifiable Info (PII), and have a reasonably good sense of where it is collected and how it is handled;
• Record and track data incidents and more quickly respond to them, thus mitigating possible corporate and individual risk; and
• Educate the workforce to be more aware of privacy considerations and obligations.

Summary

*Privacy by Design* is within reach of any organization. One of the objectives of this case study was to inspire the reader to adapt one or more of the ideas used at IBM for their own *PbD* program.

IBM, in meeting its privacy assessment and risk management goals, ultimately recognized that the implementation of The 7 *PbD* Foundational Principles created value beyond its original goals. *PbD* pointed out the importance of employee education, technology and, most of all, taking a proactive management approach.

This experience has shown that:

• Even as new technology appears to inspire new privacy risks, at its core, technology is essentially privacy neutral. What is generally at issue is the manner in which it is implemented. In fact, in the very best tradition of *PbD*, one sees the positive-sum manner in which technology may be used to foster an environment that meets both business objectives and privacy needs;
• Some data breaches are inevitable. Quick and effective response to them characterizes a best practice;
• It is critically important to relentlessly pursue a high standard of employee education. Attention must be paid to high-quality materials which are thoughtfully delivered, as well as to tracking employee participation and performance. In this fashion, senior management’s commitment to a culture of privacy may be successfully instilled within the workforce from the customer-facing, front-line staff to those in the back office; and
• Ultimately, successful implementation of tools rooted in The 7 *PbD* Foundational Principles becomes a self-fulfilling prophecy. At IBM, attentiveness to privacy is now embedded throughout the global enterprise.
IBM is pleased to share these experiences and hopes they will help other organizations take their privacy initiatives to the next step. After all, the more proficient organizations become at managing personal information, the more effective society will be at protecting privacy. Moving from privacy policies to disciplined and efficient practices that embody The 7 PbD Foundational Principles is critical to achieving the promise of an increasingly information-rich and interconnected planet.