IDIS (2010) 3:405–413
DOI 10.1007/s12394-010-0053-z

Privacy by Design: essential for organizational accountability and strong business practices

Ann Cavoukian · Scott Taylor · Martin E. Abrams

Received: 7 December 2009 / Accepted: 16 March 2010 / Published online: 4 June 2010

Abstract An accountability-based privacy governance model is one where organizations are charged with societal objectives, such as using personal information in a manner that maintains individual autonomy and which protects individuals from social, financial and physical harms, while leaving the actual mechanisms for achieving those objectives to the organization. This paper discusses the essential elements of accountability identified by the Galway Accountability Project, with scholarship from the Centre for Information Policy Leadership at Hunton & Williams LLP. Conceptual *Privacy by Design* principles are offered as criteria for building privacy and accountability into organizational information management practices. The authors then provide an example of an organizational control process that uses the principles to implement the essential elements. Initially developed in the '90s to advance privacy-enhancing information and communication technologies, Dr. Ann Cavoukian has since expanded the application of *Privacy by Design* principles to include business processes.

Keywords Fair information practices · Organizational accountability · *Privacy by Design* · Privacy assurance

Foreword

The proposition that "privacy is good for business" is one that is enshrined in all Fair Information Practices (FIPs) around the world and, through them, in the many laws and organizational practices upon which they are based. By setting out universal

A. Cavoukian
Information & Privacy Commissioner of Ontario, Canada, Toronto, ON, Canada

S. Taylor
Hewlett-Packard Company, Palo Alto, CA, USA

M. E. Abrams (✉)
Centre for Information Policy Leadership, Hunton & Williams LLP, Richmond, VA, USA
e-mail: mabrams@hunton.com

principles for handling personal data, FIPs seek to ensure the privacy of individuals and to promote the free flow of personal data and, through them the growth of commerce.

The enduring confidence of individuals, business partners and regulators in organizations' data-handling practices is a function of their ability to express the FIPs' core requirements. These are: to limit collection, use and disclosure of personal data; to involve individuals in the data lifecycle, and to apply appropriate safeguards in a continuous manner. These requirements, in turn, are premised upon organizational openness and accountability. The ultimate results—which are highly desirable—include enhanced trust, improved efficiencies, greater innovation, and a heightened competitive advantage. Privacy *is* good for business.

But the early FIPs drafters and adopters had in mind large mainframe computers and centralized electronic databases. They could never have imagined how leapfrogging revolutions in sensors, bandwidth, storage, and processing power would converge into our current hyper-connected "Web 2.0" networked world of ubiquitous data availability.

It has become trite to observe that data is the lifeblood of the new economy, but who today can truly grasp how large the arteries are becoming, how they are multiplying, where they may lead, and to what end? Everywhere we see near-exponential growth of data creation, transmission, use and storage, by an ever-expanding universe of actors, somewhere out there in the opaque "cloud." Most of this data is personally-identifiable. And most of it is now controlled by someone other than the individual himself or herself. Thanks to new information flows, today we enjoy unprecedented and nearly unimaginable new services and benefits, but these have been accompanied by unprecedented and once unimaginable privacy threats and harms. Some say that privacy is effectively dead or dying in the information age. We say that it is not, but it *is* rapidly changing shape.

The need for organizational accountability remains constant—indeed, it has become more urgent today than ever before. What is changing are the *means* by which accountability may be demonstrated, whether to individuals, regulators or to business partners. Beyond policy statements, what is needed now are more innovative and more robust methods for assuring that personal data is, in fact, being managed responsibly.

There are many paths to enhanced accountability and assurance, typically involving a mix of technology, policies and practices, and of law and regulation. More than ever before, a comprehensive and proactive *Privacy by Design* approach to information management is called for—one which assures an end-to-end chain of custody and responsibility right from the very start.

Introduction

Professor Paul A. Schwartz recently wrote:

> Companies are now putting internal policies in place, centered on forward looking rules of information management and training of personnel. Such policies are, at the very least, a necessary precondition for an effective accountability regime that develops a high level of privacy protection.[1]

[1] "Managing Global Information Privacy: A Study of Cross-Border Data Flows in a Networked Environment," Paul A Schwartz, a working paper by The Privacy Projects, October 2009.

An accountability-based regulatory structure is one where organizations are charged with societal objectives, such as using information in a manner that maintains individual autonomy and protecting the individual from social, financial and physical harms that might come from the mismanagement of information, while leaving the actual mechanisms for achieving those objectives to the organization. One of the best conceptual models for building in the types of controls suggested by Professor Schwartz is *Privacy by Design*. The best in class companies in Schwartz's study, "Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment," are using *Privacy by Design* concepts to build business process that use personal information robustly with clear privacy-protective controls built into every facet of the business process. In other words, *Privacy by Design* and accountability go together in much the same way that innovation and productivity go together.

Accountability is the governance model that is based on organizations taking responsibility for protecting privacy and information security appropriately and protecting individuals from the negative outcomes associated with privacy-protection failures. Accountability was first framed as a privacy principle in the OECD Privacy Guidelines.

The Centre for Information Policy Leadership at Hunton & Williams LLP has recently acted as secretariat for the Galway project that defined the essential elements of accountability.

The conceptual model, *Privacy by Design*, was developed by Ontario Privacy Commissioner Ann Cavoukian in the 1990s to address the development of technologies, but she has since expanded it to include business processes.[2]

Hewlett Packard is in the midst of implementing an accountability tool built on both accountability principles and the key concepts of *Privacy by Design*. HP's accountability tool is an example of the trend described by Professor Schwartz.

This paper discusses the essential elements of accountability, *Privacy by Design* principles, and provides an example of a control process that uses the principles to implement the essential elements.

Convergence of accountability and *Privacy by Design*

Accountability as both a basic privacy implementation and enforcement principle dates to the approval of the OECD Privacy Framework in 1980. But it is only today that the privacy community is beginning to understand what is meant by accountability-based privacy governance, and how it impacts the structuring of a privacy program. The growth of Binding Corporate Rules in the European Union, Cross-Border Privacy Rules in APEC, Safe Guard concepts in the United States, and data transfers compliant with the Personal Information and Electronic Documents Act (PIPEDA) in Canada has made clear direction on accountability crucial. The Galway project published a paper called "Data Protection Accountability: The Essential Elements," in October 2009 that enumerated five essential elements for

[2] "*Privacy by Design*," Ann Cavoukian, Ph.D., January 2009.

accountability. The paper was developed with a distinguished group of privacy experts from privacy enforcement agencies, government, academia, civil society and business, and facilitated by the Office of the Irish Data Protection Commissioner, and chaired by the Centre. The essential elements make it clear that accountability comes from privacy protections based on commitment to a program where privacy is built into all business processes.

Over a decade ago Ontario Privacy Commissioner Ann Cavoukian began discussing the virtues of building privacy into technology from the start. She calls that concept "*Privacy by Design*." While *Privacy by Design* began as a technology concept, it has evolved into a conceptual model for building an entire privacy program.

The fact is that *Privacy by Design* and accountability go together like innovation and high productivity. You can have one without the other, but it is hard.

A number of companies have been building programs where privacy is built into core business processes. One can find them in many industries and both business to business and business to consumer industries. Hewlett Packard has spent the last three years building a program called the "Accountability Model Tool" that integrates the technological concepts of *Privacy by Design* with the organizational commitment required for accountability. The accountability tool is now being implemented in the HP businesses that serve customers in 170 countries through 400,000 employees. This paper will describe accountability's essential elements, the components of *Privacy by Design* and will use the HP "Accountability Model Tool" as an example of how leadership companies are building privacy in.

The essential elements of accountability

Accountability has a strong basis in privacy law and oversight. The Organization for Economic Cooperation and Development ("OECD") included accountability as principle eight in the Guidelines. Accountability is principle nine in the Asia Pacific Economic Cooperation forum ("APEC") Privacy Framework. It is principle one in the Model Code for the Protection of Personal Information (incorporated into Canadian law), and is a principle in the joint proposal drafted for consideration at the 31st International Conference of Data Protection and Privacy. However, none of those documents defined accountability as it applies to privacy.

The Centre for Information Policy Leadership at Hunton & Williams LLP, in a process facilitated by the Office of the Irish Data Protection Commissioner, brought together a group of experts to consider the essential elements of accountability in a project called the Galway Accountability Project. The Galway project held two experts discussions in Dublin, Ireland, the second sponsored by the OECD and the Business and Industry Advisory Council to the OECD. For the purpose of those discussions the group used the following working definition of accountability:

> Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions.

For an organization to have the capabilities to demonstrate its willingness to meet expectations based on law and organizational promises, and to have confidence in its ability to be answerable, the organization must have all aspects of privacy and information security under control. This is reflected in the essential elements of accountability:

1. An organization's commitment to accountability and adoption of internal policies consistent with external criteria
2. Mechanisms to put privacy policies into effect, including tools, training, and education
3. Systems for internal ongoing oversight and assurance reviews and external verification
4. Transparency and mechanisms for individual participation
5. The means for remediation and external enforcement.

To be an accountable organization a company must have rules that are based on an external measuring stick such as data protection laws, industry self regulatory guidance, or guidance such as the OECD guidelines or APEC principles. Those policies must then be committed to by the organization at the highest level. The organization must have all the pieces in place to assure that the people who work at (employees) and for the organization (vendors) can be successful in implementing its policies and commitments. Furthermore, the organization must have internal measurement devices in place to assure the actions meet the words, and an external process to verify performance.

Privacy by Design is a process map for putting the essential elements of accountability into effect.

***Privacy by Design*: seven foundational principles**

Ontario Privacy Commissioner Ann Cavoukian has written that *Privacy by Design* is achieved by building fair information practice principles ("FIPs") into information technology, business practices, and physical design and infrastructures. This links with the accountability concepts in two ways. First the essential elements require that policies and practices must be based on external criteria. FIPs are the sum and substance of OECD and APEC privacy guidance, built into the European Union Data Protection Directive, and Canada's PIPEDA. They are examples of the external criteria referenced in the essential elements. Second, is the concept that the FIPs need to be built into all the processes from technology development to the physical structure of facilities. This too is required by the essential elements.

Dr. Cavoukian has also written that *Privacy by Design*'s objectives may be accomplished through adoption of seven foundational principles.

The Foundational Principles are listed below and linked to the essential elements of accountability:

1. ***Proactive not Reactive; Preventative not Reactive*** Proactive not reactive speaks to the accountability concept of having all the privacy policies as well as mechanisms in place so trained practitioners can observe and resolve privacy issues before they turn into problems.

2. ***Privacy as the Default*** Accountability requires clear organizational rules with an explicit commitment to the policies that are the basis for those rules. Those rules will make clear that information should only be collected and used in a manner that is respectful of individual expectations and a safe information environment.
3. ***Privacy Embedded into Design*** Accountable business processes work best when privacy is embedded into design. This would be part of the mechanisms to implement policies.
4. ***Full Functionality—Positive Sum, Not Zero-Sum*** Organizations that understand privacy and bake privacy in have a better comprehension of the risks to both the organization and to individuals. Organizations that build privacy in know how to create economic value while protecting individual privacy. The Centre purports that clear privacy rules and methodologies create confident organizations that do not suffer from reticence risk.
5. ***End-to-End Lifecycle Protection*** End-to-end lifecycle protection informs the accountable organization that it must build privacy into every process from the assessment before data is collected to the oversight when data is retired.
6. ***Visibility and Transparency*** Principle six requires an organization to be open and honest with individuals. The accountable organization stands ready to demonstrate that it is open about what it practices, stands behind its assertions, and is answerable when questions arise. The accountable organization provides the information necessary for individuals to participate consistent with the OECD individual participation principle. This is echoed in the *Privacy by Design* visibility and transparency principle.
7. ***Respect for User Privacy*** Lastly, the accountable organization must collect, use, store, share and retire information in a manner that is consistent with respect for the individual's privacy.

Leadership companies are demonstrating *Privacy by Design*

In the course of the Centre's research we looked at leadership companies' information policy policies and practices. We saw information aggregators with excellent assurance review processes, software companies that build privacy protections into processes, and outsourcing companies with excellent checks and balances. "Managing Global Information Privacy: A Study of Cross-Border Data Flows in a Networked Environment" by Paul Schwartz looked at the processes that six companies had for protecting privacy in an application that required data to cross borders. Professor Schwartz found all of the organizations to have very professional processes to assure data is used and protected appropriately.[3]

While there are many corporate examples of *Privacy by Design*, Hewlett Packard makes an interesting case study since they are in online retail, indirect retail, business-to-business, and services.

[3] "Managing Global Information Privacy" is available on the OCED website (www.oecd.org) and The Privacy Projects, a NGO that sponsored the research.

Privacy by Design—an HP example

Globalization and new technologies are fundamentally changing how companies communicate and market to customers and prospects. It changes both the opportunities and the risks for individuals and organizations. Many of these technologies, including Web 2.0, user-generated content, and social media are straining traditional frameworks. And as the collection of data becomes more ubiquitous, data mining, analytics and behavioral targeting are growing more and more common and complex.

Laws and regulations often lag behind the practical realities of new technologies. This points to the fact that companies need to develop mechanisms that balance the tensions of using information robustly, yet ensure responsible decision making. Regulators and advocacy organizations are also looking to companies to demonstrate their capacity in upholding obligations and that their use and management of data is under control.

The *Privacy by Design* concepts, originally conceived by Commissioner Cavoukian, can be instantiated within a company in many ways. In an attempt to drive accountability throughout the enterprise, and ensure privacy considerations are taken into account at the earliest stages of a product's lifecycle, HP has developed a tool that guides employees.

As this paper articulates, accountable practices can be broken down into three major categories: 1. Policies and Commitments, 2. Implementation Mechanisms, and 3. Assurance Practices. It is in the development of implementation mechanisms where *Privacy by Design* becomes critical. Employees of an organization must understand how to put policies, obligations, and values into effect. And to minimize business investment, reputation and compliance risks, employees need to consider privacy principles prior to design.

If a product or program is broken down into simple stages, it becomes clear when *Privacy by Design* guidance versus assessment needs to be applied. In the stages of Design and Development, the Privacy Office should provide proactive guidance so that privacy considerations can inform the planning stage. This is often missed and can result in a program being delayed or cancelled based on later privacy concerns.

Early guidance related to privacy becomes a tremendous value added to the organization. If caught early, privacy pitfalls can be avoided and good privacy practices embedded into the design of the program.

In the Pre-deployment, Deployment, Maintenance, and End-of-life stages, the Privacy Office needs to do more than just guide—they need to provide robust assessment mechanisms to ensure compliance with local laws, obligations, policies, and company values.

The assessment results should be documented and reviewed by the Privacy Office, consultation provided as necessary, and ultimately approved prior to deployment. After product or program launch, triggers should exist to ensure deployment was consistent with expectations and that end of life actions are taken when appropriate.

For many years, HP has been managing this *Privacy by Design* lifecycle through education, training, and encouraging employees to engage their privacy account

manager at the early stages of design and development. As successful as this can be, it relies on employees thinking about privacy at the right time, knowing who to contact, and not feeling intimidated.

To solve these challenges and take *Privacy by Design* to a new level, the HP Privacy Office partnered with research scientists in HP Labs to develop a solution called the Accountability Model Tool. It combines the guidance in HP's existing Privacy Rulebook with a set of contextual, dynamically-generated questions. These two knowledge bases are connected through a sophisticated rules engine to help guide employees.

It allows employees and teams—working on simple marketing campaigns or complex product solutions—to see what privacy considerations need to be designed into their program. As described above, it works in both a guidance mode and in an assessment mode—depending on the lifecycle stage of the program.

Through company policy, employees who are collecting or using PII are required to assess their programs using this tool. It is easily accessible from the internal Privacy Intranet site. Using their digital badge they are authenticated and their basic contact and organizational information is automatically populated in the tool. All of their past projects are also accessible. This is important if an employee changes jobs or leaves the company so the Privacy Office knows which organization remains accountable for a program.

The tool begins by asking simple questions about the nature of their project. If it involves the collection or use of PII, they are presented with further contextual questions. As they answer each question, the next set of questions is dynamically generated based on how they answered prior questions. This is a critical component of success. The Privacy Office has found that each employee understands his or her area of expertise (e.g., e-mail marketing, product development, or employee relations), but when guidance and rules are not contextualized to their area of work, it becomes a daunting task for them to sift through hundreds of pages of rules or guidance and know how to apply them to their program. This tool is meant to narrow the context into exactly what they are doing and provide the associated guidance.

By asking employees contextual questions—and linking their answers immediately against the rules database—the tool not only guides, but educates the employee on good privacy practices. For each question, terms are defined by using text rollovers and help is provided that links the employee directly into the HP Privacy Rulebook. They can also check a box that says "Question is Unclear." This allows the Privacy Office to track trends and improve the delivery of questions if patterns evolve.

The tool takes the employee through a series of questions related to the profile and nature of the project, data sources and flows, transparency, compliance, and indicators of any issues that might arise or surprise the data subject. Once the employee has completed the questions, a report is generated that shows an overall rating, as well as areas of compliance and non-compliance.

For areas of non-compliance, reasons are provided, including links to further information and checklists that can be used to achieve compliance.

Once the employee has made the appropriate modifications, he or she can submit their report to the HP Privacy Office where it will be reviewed and archived.

They are attesting to the truth and accuracy of their statements and will be held accountable. For any areas of concern, the Privacy Office must approve the program prior to deployment.

Once approved, the program information is warehoused in the database. It is maintained for future use as well as a trigger for ongoing assurance monitoring. This database of projects provides a real-time dashboard for the Privacy Office, allows improved ongoing communications and ensures that if laws or regulations in a country change that programs can be modified as appropriate.

This is a new program for HP and has just been deployed. It is a valuable tool along with ongoing efforts in training, implementation standards, compliance management, and audit. It achieves Commissioner Cavoukian's concepts for *Privacy by Design* in a manner that is systematic, predictable and repeatable—and ultimately will drive a richer culture of privacy within the enterprise. It also will enable HP to better demonstrate commitment and capacity in upholding privacy promises and obligations.

Conclusion

In this paper, we have seen an excellent example of how enhanced privacy accountability and assurance can be achieved within an organization by applying *Privacy by Design* principles, in a thoroughgoing manner.

So imperative today are the goals of enhanced accountability and assurance, so universal are the PbD principles, and so diverse are the contexts within which these principles may be applied, that the future of privacy in the 21st century information age may be limited only by our collective imagination and will.

There are virtually infinite ways by which organizations can creatively "build privacy in" to their operations and products, to earn the confidence and trust of customers, business partners and oversight bodies alike, and to be leaders in the global marketplace.

We need to acknowledge and celebrate these innovations and successes, and steadily build upon them.

Acknowledgements The authors wish to acknowledge Fred Carter, Senior Policy and Technology Advisor, Policy Department at the Information and Privacy Commissioner's Office, Ontario, Canada for his input on this paper, as well as Susan Smith, Americas Privacy Officer, Hewlett-Packard Company and staff at The Centre for Information and Policy Leadership at Hunton & Williams LLP.