Privacy by Design

(Volume 21, Number 3)

By

Heather A. Smith
James D. McKeen

Deloitte.

Queen's
SCHOOL OF BUSINESS
ACADEMIC EXCELLENCE. EXCEPTIONAL EXPERIENCE.

Introduction

This year’s CIO Brief theme is “Enhancing the Customer Experience with Technology”. In our first meeting, we explored "Transforming Customer Experience at UP Express". In the second session, we looked at empowering and mobilizing customers. This third session examined the role of privacy in the customer experience. The Brief invited Sylvia Kingsmill, National Partner and Digital Privacy Leader at Deloitte, of Deloitte's Enterprise Risk Group and Kathleen Champagne, AVP Global Privacy Operations and Special Projects at TD Bank, to discuss this topic with the group.

What the Chief Privacy Officer wants the CIO to Know: Part 1

"The privacy landscape has changed dramatically in recent years, which has resulted in an evolution of the Chief Privacy Officer (CPO's) role," said Sylvia. With increasing regulatory scrutiny by Privacy Commissioners, new digital privacy laws, privacy class action lawsuits launched against companies that have disregarded privacy and security issues, and new boardroom conversations about digital strategy mean that more attention is now being paid to IT-privacy risk. Therefore, today's CPO should be involved in helping shape IT strategy, understanding customers, developing privacy-enhancing solutions, applying customer learnings to operations, prioritizing technology and analytics investments while protecting privacy and security to reap the benefit of digital investments. "This is an opportunity for the CIO and CPO to collaborate on privacy issues and break the traditional silos," she said.

"Privacy is *not* about secrecy," she explained. "It's not about having something to hide." It *is* about control and offering the customer the right to determine how their information is used and shared once it’s collected. The right to control information about oneself is referred to as “informational self-determination” – a concept that can help reframe the privacy conversations between the CIO and CPO when launching new products and services. Studies show that customers are willing to share more information about themselves with brands they trust to protect their personal information. There is a tremendous opportunity for value creation in data capture which must be balanced with the need to protect the information to give a seamless customer experience from a privacy perspective. Business should be enabled by IT to drive innovation and this can only be achieved by viewing privacy as a risk management issue.

This means that privacy and security can’t be an afterthought – it must be integral throughout the design process. "We need to have these conversations upfront, during the requirements gathering and development phase, rather than retrofitting our IT systems. This is a more cost efficient and effective approach to managing privacy risk, resulting in customer loyalty and trust – an approach we refer to as “Privacy by Design," she concluded.

In a landmark resolution passed in 2010 by global Data Protection Authorities, Privacy by Design has been endorsed as the international standard for privacy protection: http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy.

It is based on seven common sense, simple-to-follow Foundational Privacy Principles:

1. **Proactive not reactive**; preventative not remedial. Anticipate privacy invasive events by being prepared and understanding your threat landscape.

2. **Privacy as the default setting.** Privacy protection should be automatic, giving consumers choice on how they want their data shared.

3. **Privacy embedded into design.** Don’t bolt privacy on after-the-fact.

4. **Full functionality: positive sum not zero-sum**. All legitimate business uses of the information should be accommodated in a fair manner. Create a win-win for both consumer and organization.

5. **End-to-end security: full lifecycle protection**. Security protection is applied from collection to dispositions of the data.

6. **Visibility and transparency**. Keep it open and user-centric -- trust but verify!

7. **Respect for user privacy: keep it user-centric.** Empower user-friendly options.

Sylvia's Data Protection and Privacy practice has developed a Privacy by Design assessment framework that aligns to these principles, which includes 29 measurable privacy assessment criteria and 107 illustrative privacy control activities organizations can assess and certify against. The Privacy by Design control framework is based on harmonized international privacy laws and best practices and is publicly available at: http://ryerson.ca/content/dam/pbdi/Certification/Privacy%20by%20Design%20Certification%20Program%20Assessment_Privacy%20Controls%20Framework%2020150716.pdf

In her closing remarks, Sylvia addressed two prevalent privacy myths:

- ***Privacy is really the CPO's problem.*** IT personnel should never assume that their project has no privacy implications or that there will be no privacy show-stoppers because the CPO is involved. "Everyone in the organization is in this together when relying on data as a business-critical asset," Sylvia said. "It's important to clearly document roles, responsibilities and accountabilities, to define risk ownership, and formalize a privacy governance model that defines how data should be protected."

- ***Privacy is really a legal problem.*** "We should move away from thinking about privacy as a tick-the-box compliance exercise but rather, as a business issue," she said, "and integrate privacy risk management into strategic planning and resource allocation." Privacy risk and return can be easily analyzed when and privacy and security-enhancing features built into the process, technology, and culture when rolling out all IT initiatives.

Sylvia believes that the CIO should proactively collaborate with the CPO to drive innovation by adopting privacy and security-enhancing technologies. Some important challenges that can be overcome with this approach are: managing the risk of re-identification where big data technologies can enable easy identification of individuals from supposedly anonymized data sets; doing away with creepy customer profiling and tracking by capturing layered and/or just-in-time consumer notices that are transparent and easily understood (pro-consumer); ensuring strong access controls and security protections are built right into the architecture to avoid data breaches; and maintaining accountability for personal information through good privacy governance, even when the data is in the hands of service providers and agents.

What the Chief Privacy Officer wants the CIO to Know: Part 2

Kathleen Champagne comes from an eclectic background with experience in customer support, marketing, project management, enterprise initiatives, compliance, and now privacy. "There are two significant privacy risks that every CIO must care about," she said. The first is unauthorized third party access to company systems resulting in the disclosure of personal information. The second is employees or service providers inappropriately using company systems or confidential information, including personal information. "Companies spend millions of dollars addressing the first risk, and very little on the second," she said. Recently, there have been cases in the news where health care workers and bank tellers have leaked information to the public or acted on confidential information out of a personal grudge. "This is my biggest worry at present."

She would like CIOs to consider how they could make it more difficult for a person to see everything in a record by limiting it to only the information needed. In addition, she would like to find algorithms to automatically manage 80% of information in this way and then develop protocols to limit the risk involved with the other 20%. She also wants to work with IT to develop proactive systems that would raise red flags about employees doing something odd and systems that would provide a detailed history of who accessed what and when.

At present, her top areas of concern at present are:

1. **Improper vetting** of vendors, suppliers, contractors, agents and partners. "Our contracts should not just be about cost and time but *how* they will do the job. And we need to continually monitor them to see they are doing it properly," she said.

2. **Failure to obtain required consent.** For example, anti-spam legislation requires both consent and the ability to withdraw consent. Some companies are currently advertising based on a person's location and mobile behavior, but don't offer ways to give consent to ads or ways to withdraw. "We need ways to demonstrate express consent and then offer ways to withdraw it," Kathleen said.

   Members expressed frustration with current legislation and Kathleen agreed that there are ways to make it work better and promote e-commerce. "We will have an opportunity to review this legislation in the future and make it better, but our current problems seem simple compared to where we are going," she said. For example, companies are beginning to use profiling and analytics to learn much more about their customers and legislation is not keeping pace with this work. "This is the reason why we need to think about privacy up front and not do the bare minimum. We also need to find out about and adopt best practices in this area," she said. "It's not about what we can't do but what we *can* do. We must work with our customers to find out when customer service and profiling gets creepy. I am personally terrified about where analytics could take us."

3. **Failure to assess the impact of privacy requirements on new products in a timely manner.** This affects programs such as BYOD.

Lack of awareness of changing geographic privacy regulations that affect how business can be conducted. For example, general data laws are very strict regarding EU residents no matter where they are. And the US is also seizing data from abroad. "Governments will get data when they need it," Kathleen concluded. "However the environment of privacy is moving at breakneck speed and we need to pay attention to the *potential* of these laws. If we don't, there will be lots of rework."

A New Technology for Authentication

Dave Rai, of Nymi then presented a new technology for biometric identification, which he is piloting with the TD Bank. "The Nymi Band is a wearable authenticator that increases both security and convenience through continuous proximity-based access control," he explained. Users wear a wristband that authenticates their

HeartID, which is based on an electrocardiogram. They can log in and authenticate passively as long as the band stays on their wrist. "Our heart rhythms are unique," Dave said. "Unlike today's picture ID cards, the Nymi band continuously identifies the wearer. Although it doesn't solve all data access problems, it does solve the problem of "who I am" with authentication data that does not reside in the cloud and that can tie into an identity management system."

Members asked about the band's security. Nymi uses a proprietary cryptographic layer running on top of Bluetooth to ensure security and enable one-to-many communication. The continuous confirmation of identity makes it very difficult for one person to impersonate another. The combination of a biometric means of authentication with a wearable ensures persistence of identification and this creates trust.

Some possible uses for the band include: creating secure sessions for developers; ensuring appropriate physical access to facilities; providing multifactor identification when signing into a VPN; enabling contactless payments; fitness tracking; locking and unlocking terminals for frontline staff; providing single sign on, and offering geo-presence identification for legal purposes. The band is being piloted with a large enterprise to test some of these uses. Members asked if staff have any anxiety about wearing a band. "No," said Dave, "because fitness bands are now in fashion."

Using Wearables to Monitor Social Behaviour

Sylvia Gonzalez of Deloitte reported on an experiment her firm is undertaking with Humanyze, a leader in the field of social sensing and people analytics. In this case, Deloitte employees in their St. John's office wore a device that enabled them to see their communication patterns relative to those of others. It showed that with greater awareness of personal communication patterns over time, overall communications patterns changed to include more interaction time and more exploration with other teams. The company has also used it to increase networking and cohesion in its Global Analytics Team and partners are now using it in several offices worldwide.

Members asked if everyone likes using this technology. "Employees are allowed to opt in or out," said Sylvia. However, members pointed out that employees cannot be deemed to give consent to such technologies since they are "under duress".

Discussion

Now that technologies are able to pick up more information than in the past, does this change our concept of privacy? This is both a challenge and an opportunity, said the panel. Privacy needs to be balanced with other issues. The key to doing this successfully is providing choice and control.

How can privacy keep up with changes in technology? Our policies can't change fast enough so it's important to understand the following questions: What information are we giving up and to whom? What's being done with this information? Who has access to it? What are third parties doing with it? Most people don't understand these issues and even well-educated people are giving up their data with understanding them. Companies need to focus on what is happening practically with data. "We can have a great policy but we then need to operationalize it," said Kathleen. "People are our weakest link."

Should CPOs focus on how to limit liability and how much data is accessed? "CPOs need to stop being the privacy police," said Kathleen "and work with IT personnel to help them understand how a CPO can help them. We should be more about enablement and less about compliance." Protecting personal data can be a benefit to an organization and instill trust in a company. A good test of a practice is whether it is better for the consumer. In short, good privacy practices can be a competitive advantage.

What is the relationship between security and privacy? Privacy is about information handling – what is collected and how it is used, said the panel. Security enables privacy by preventing unauthorized access.

On average, how well does IT understand privacy issues? "IT is aware of privacy issues but doesn't always understand the repercussions of certain decisions and designs," said Sylvia. "Our skill set in this area is not deep enough." Changes are being made in some industries, notably healthcare, but there is a big language barrier between all the different IT and business groups that inhibits clear understanding of privacy considerations. "Some groups 'get it'", said Kathleen "and others just think of privacy as a big cost."

Concept

CIO Brief 2.0 is an group of CIOs from leading edge organizations who meet to exchange best practices concerning IT management strategy. The CIO Brief 2.0 is organized by James McKeen and Heather Smith, Queen's School of Business, in partnership with Deloitte Canada. See www.ciobrief.ca.

Recent Reports

Big Data and Business Intelligence
IT and the Board of Directors
CIO as Innovator
The Process of Idea Generation
Innovation Design and Development
IT Talent Management
Redefining IT: Cultural Change and Business Alignment
Systems of Engagement
Becoming Agile
The CIO-CMO Relationship
Transforming the Customer Experience at UP Express
Empowering and Mobilizing Customers

Participating Organizations

ADT Security Services
Bayshore Heatlthcare
BMO
Black & McDonald
CAA
Cadillac Fairview
Canadian Tire
Comark
Elections Ontario
EMC
Empire Financial Group
EQAO
Fairmont Raffles Hotels
GTAA
Kanetix
Kik
LCBO
Loblaw
Alcohol and Gaming Commission of Ontario
Metrolinx
Mt. Pleasant Group
Ontario Teachers Pension Plan
OPTrust
Parmalat
RBC
SCI Group
ScotiaBank
Sony Canada
TIFF
UP Express
Weston Foods

Membership

Membership is by invitation only. Please direct inquiries to James McKeen at jmckeen@business.queensu.ca.

ACADEMIC EXCELLENCE. EXCEPTIONAL EXPERIENCE.