Managing Privacy Risk in the Age of the Internet

Sylvia Kingsmill, National Partner
Data Protection and Digital Privacy Leader
November 12, 2015
Let’s talk about privacy….
What is the Internet of Things (IoT)?

- Automotive / Transportation
  - Dealership of the future
  - Remote diagnostics
  - Fleet management
  - Smart car

- Energy & Resources
  - Smart grid
  - Wellhead optimization
  - Autonomous Mining

- Manufacturing / Supply Chain
  - Wireless factory
  - Preventative maintenance
  - Supply chain

- Military
  - Connected battlefield
  - Supply chain

- Financial Services
  - Perf-based Insurance
  - Personalized risk profiles
  - Online banking
  - Digital wallet

- Healthcare/Lifesciences
  - Remote monitoring
  - Patient experience
  - Equipment monitoring
  - Patient care
  - Medical devices
  - Bio wearables

- Consumer
  - Wearables
  - Smart thermostat
  - Smart home
  - Smart alarm system

- Retail / Vending
  - Tailored offers
  - Inventory management
  - Checkout optimization
  - Supply chain

- Smart Cities
  - Smart lighting
  - Smart parking
  - Smart waste
  - Smart meter

“Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion” – Dave Evans, CISCO
The information value loop – creating value from information

**Create** | the use of sensors and data to generate information about a physical event or state

**Communicate** | the transmission or information from one place to another via networks

**Aggregate** | the gathering together of information created at different times or from different sources

**Analyze** | the discernment of patterns or relationships among phenomena that leads to descriptions, predictions, or prescriptions for action

**Act** | initiating, maintaining, or changing a physical event or state – machines can make decisions based on aggregate data that is analyzed

© Deloitte LLP and affiliated entities. | Managing Privacy Risk in the Age of the Internet
Smart Cars

• Fully self-driving cars are expected to be on the market within 10 years
• Capable of sensing their environment and navigating without human input using technologies such as radar, GPS, and computer vision

Benefits

• Sensors on a car can notify drivers of dangerous road conditions
• Safety and convenience by taking human error out of the equation
• Wireless software updates, no need for dealership service
• Real time vehicle diagnostics to drivers and service facilities
• Automatic alerts to first responders when airbags are deployed or accidents occur
• Fully connected with smart phones for convenience
Wearables

- Wearable technology includes a wide variety of devices from smart watches and glasses to smart clothes.
- Wearable technology enables a wide range of activities, which in turn enables a highly integrated customer experience.

Benefits

- Enables new services that suit changing customer lifestyles
- Enables assessment of customer preferences which contributes to new and better software and technology
- Reduce costs from health insurance companies for good health behaviour
- Vital signs can be monitored without having to be at a doctor’s office
- Connected health care devices can provide treatment options that can be independently managed
- Ease of sharing information to doctors or nurses, which can improve disease prevention, better drug management, and drive costs down due to a more efficient health care system
The Digital Enterprise – our evolving version of where business is heading in the next few years. Already, mobile advances have put incredible technology in everyone’s hands. Social networks enable people to connect in ways never before possible. The cloud is drastically reducing the costs associated with hardware and data infrastructure, while data storage capabilities grow ever larger and ever cheaper. Data analytics can now make sense of vast amounts of data to provide valuable, actionable insights.
The connected consumer
New boardroom discussion

**CEO** Shaping business strategy infused with technology—advising and executing on realities of existing capabilities, and the potential of emerging trends.

**CFO** Framing initiative investments, operations, delivery, and budget in terms of risk management and return on assets.

**CCO** Understanding, prioritizing, and addressing pain points and inefficiencies in analytics, business processes, and operations—retooling how work gets done.

**CMO** Partnering to implement new marketing tools with hooks into back-office data and transactions, while retooling to offer agile delivery for new digital solutions.

**CHIEF PRIVACY OFFICER** Elevating privacy to the boardroom agenda, protecting data as a strategic asset for profitability, effective and efficient operations, growth and innovation.

**CHIEF DIGITAL OFFICER** Collaborating to define a vision and roadmap, provide integration, security, and data services, and drive sustainable roll-out of digital services.

**CHIEF DATA OFFICER** Planning and execution of new capabilities and governance of internal, external, structured, and unstructured data sources and surrounding tools.

**CHIEF INNOVATION OFFICER** Seeding technology-based innovation ideas while complementing the “art of the possible” with the “realities of the feasible.”

**CHAIRPERSON**
Weighing the risks

Benefits

• Increased profitability
• Enhanced customer experience
• Improved productivity
• Reduced costs
• Improved process
• Enhanced safety
• Increased efficiencies

Risks

• Privacy and security
• Stakeholder acceptance
• Usability
• Standardization
• Legal liability

Value generated by new technology
Connected car – Who is in the driver’s seat?

What is being collected?

- Customer account data
- Vehicle performance data
- Driver behaviour data
- Biometrics and health data
- Location data
- Personal communications (voice, text, email, social networking)
- Web browsing data, stream audio or video content
- Personal contacts and schedules

“There’s plenty of people out there saying: Give us all the data you’ve got and we can tell you what we can do with it.” Ian Robertson, BMW Board Member for Sales and Marketing

Phillipa Lawson, FIPA Report, 2015
Privacy Risks

Increased connectivity between devices and the Internet may create a number of security and privacy risks:

- Enabling unauthorized access and misuse of personal information
- Facilitating attacks on other systems
- Creating safety risks
- Lack of security in wearables when information is being transmitted
- Direct collection of sensitive personal information (geolocation, financial account information, health information, habits)
- The collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to make inferences or decisions about a person’s credit, insurance or employment

### Risks – who owns the problem?

**The legal risks:**

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property damage</td>
<td>• Property damage</td>
</tr>
<tr>
<td>Multiple vendors</td>
<td>• Multiple vendors</td>
</tr>
<tr>
<td>Negligence</td>
<td>• Negligence</td>
</tr>
<tr>
<td>Strict liability</td>
<td>• Strict liability</td>
</tr>
<tr>
<td>Warranty</td>
<td>• Warranty</td>
</tr>
<tr>
<td>Fraud</td>
<td>• Fraud</td>
</tr>
<tr>
<td>Product liability</td>
<td>• Product liability</td>
</tr>
<tr>
<td>Privacy breach</td>
<td>• Privacy breach</td>
</tr>
<tr>
<td>Misleading</td>
<td>• Misleading representations</td>
</tr>
</tbody>
</table>

**The Players:**

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chip designers</td>
<td>• Chip designers</td>
</tr>
<tr>
<td>Art manufacturers</td>
<td>• Art manufacturers</td>
</tr>
<tr>
<td>Distribution retailers</td>
<td>• Distribution retailers</td>
</tr>
<tr>
<td>App developers</td>
<td>• App developers</td>
</tr>
<tr>
<td>Raw materials seller</td>
<td>• Raw materials seller</td>
</tr>
<tr>
<td>Product seller</td>
<td>• Product seller</td>
</tr>
</tbody>
</table>
Traditional approaches to privacy

- Notice/transparency
- Choice and control (opt-out)
- Use Limitation
- Responsible and ethical use of data
- Accountability
- Data Integrity
Tracking the Tracker

“If you’re not paying for something, you’re not the customer, you’re the product being sold” – Andrew Lewis

Saks fifth avenue was visited on both Internet Explorer and Google Chrome
How law enforcement can use Google Timeline to track your every move

“The expansion of Google’s Timeline feature, launched in July 2015, allows investigators to request detailed information about where someone has been — down to the longitude and latitude — over the course of years.”

– The Intercept, Jana Winter (November 6, 2015)
Avoiding the “creep factor”
Understanding privacy risks at every stage of the connected digital consumer

Using analytics, Target Inc. took personally identifiable information and developed a list of 25 “indicator products” that could produce a “pregnancy prediction” for its female guests of childbearing age. The analytics findings enabled Target to estimate due dates in order to send coupons at specific stages of a woman’s pregnancy.

“I had a talk with my daughter” … “It turns out there’s been some activities in my house I haven’t been completely aware of. She’s due in August…”
Privacy = Control

• User control is critical
• Freedom of choice
• Informational self-determination
Enabling privacy through trust results in a win-win scenario on the value grid

“We believe the customer should be in control of their information. You might like these so-called free services, but we don’t think they’re worth having your email, your search history and now even your family photos data mined and sold off for god knows what advertising purpose” – Tim Cook, Apple CEO at EPIC Conference
Consumers’ attitudes and behaviours towards data privacy and security

Source: Consumer responses from the product consumer and executive survey on data privacy and security – Deloitte LLP, August 2014

© Deloitte LLP and affiliated entities. | Managing Privacy Risk in the Age of the Internet
Market demand for privacy
Canadian privacy trends

Privacy programs are trending towards increasing oversight and advisory services to business unit/divisions on the privacy protections that our clients and the public expect.

<table>
<thead>
<tr>
<th>Transformation</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Expectations of the public that organizations will protect their information online or in electronic format</td>
<td>Organizations are evolving their Privacy Programs enterprise-wide to embed privacy in corporate processes and technology decisions, such as in strategic business planning, project management life cycle, and enterprise risk reporting</td>
</tr>
<tr>
<td>✓ Increased capability and demand for interconnected experience</td>
<td></td>
</tr>
<tr>
<td>✓ Increased privacy awareness and expectations from the public around accountability and transparency</td>
<td></td>
</tr>
</tbody>
</table>
Then and now – how organizations manage privacy

<table>
<thead>
<tr>
<th>Privacy component</th>
<th>Past (late 90s to early/mid-2000s)</th>
<th>2010 onwards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy driver</td>
<td>Legal compliance is a big privacy driver</td>
<td>Legal compliance and digital technologies are as much of a privacy driver</td>
</tr>
<tr>
<td>Incident reporting</td>
<td>Privacy incident monitoring and reporting processes are new – organizations are just drafting their breach response protocols</td>
<td>Mature privacy incident monitoring and reporting processes; more emphasis on streamlined communications and enterprise-wide training from incidents</td>
</tr>
<tr>
<td>Training</td>
<td>Privacy training likely to be general in nature and delivered “on paper” (e.g. Employees sign a generic “privacy pledge”)</td>
<td>Privacy training likely to be customized to user groups and delivered in multiple formats (e.g. online, in-person, privacy reminders sent to users’ smart phones)</td>
</tr>
<tr>
<td>Risk identification</td>
<td>General Counsel is responsible for privacy and is often the Chief Privacy Officer (CPO); CIO is responsible for data security; it is unclear who is primarily responsible for privacy and security risk identification and mitigation</td>
<td>LOBs, Marketing, IT/IM, Risk and IA also responsible for risk identification Privacy and security are more likely to be integrated within broader risk management plans</td>
</tr>
</tbody>
</table>
Emphasis on “accountability”

The Office of the Privacy Commissioner of Canada (OPC) and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia jointly issued regulatory guidance entitled *Getting Accountability Right with a Privacy Management Program*, which sets out detailed expectations for a comprehensive privacy management program. The guidance addresses the baseline fundamentals or “building blocks” of a Privacy Program and how to monitor it on an on-going basis:

<table>
<thead>
<tr>
<th>Part A) Building Blocks</th>
<th>Part B) Ongoing Assessment and Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organizational commitment</strong></td>
<td><strong>Oversight and review plan</strong></td>
</tr>
<tr>
<td>Buy-in from the top</td>
<td>Develop an oversight and review plan on an annual basis for monitoring and assessing the organization’s privacy management program’s effectiveness.</td>
</tr>
<tr>
<td>a) Senior Management <em>endorses the program controls</em>, and <em>monitors and reports to the Board.</em></td>
<td></td>
</tr>
<tr>
<td>Privacy Officer</td>
<td></td>
</tr>
<tr>
<td>b) Privacy should be seen as <em>improving processes, customer relationship management and reputation.</em></td>
<td></td>
</tr>
<tr>
<td>Privacy Office</td>
<td></td>
</tr>
<tr>
<td>c) Organization structure supports staff to monitor compliance and foster a culture of privacy.</td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td></td>
</tr>
<tr>
<td>d) <em>Internal reporting mechanisms</em> need to be established and <em>reflected in program controls.</em></td>
<td></td>
</tr>
<tr>
<td><strong>Program controls</strong></td>
<td><strong>Assess and revise program controls</strong></td>
</tr>
<tr>
<td>Personal information inventory</td>
<td>b) The effectiveness of the Program should be monitored, periodically audited, and address the latest threats and risks, complaints or audit findings.</td>
</tr>
<tr>
<td>a) Every organization needs to determine what personal information is held and where it is held.</td>
<td></td>
</tr>
<tr>
<td>Policies</td>
<td></td>
</tr>
<tr>
<td>b) Organizations must develop and document internal policies that give effect to privacy principles established under Canadian privacy law.</td>
<td></td>
</tr>
<tr>
<td>Risk assessment tools</td>
<td></td>
</tr>
<tr>
<td>c) <em>Conducting risk assessments, at least on an annual basis,</em> is an important part of any privacy management program to ensure that organizations are in compliance with applicable legislation.</td>
<td></td>
</tr>
</tbody>
</table>

© Deloitte LLP and affiliated entities. | Managing Privacy Risk in the Age of the Internet
What is “Privacy by Design”? 

*Privacy by Design was created to reconcile the need for robust data protection with the desire for data-driven innovation.*
## Privacy by Design

### The 7 foundational principles

<table>
<thead>
<tr>
<th></th>
<th>Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Proactive not reactive: preventative not remedial</td>
</tr>
<tr>
<td>2</td>
<td>Privacy as the default setting</td>
</tr>
<tr>
<td>3</td>
<td>Privacy embedded into design</td>
</tr>
<tr>
<td>4</td>
<td>Full functionality: positive-sum, not zero-sum</td>
</tr>
<tr>
<td>5</td>
<td>End-to-end security: full lifecycle protection</td>
</tr>
<tr>
<td>6</td>
<td>Visibility and transparency: keep it open</td>
</tr>
<tr>
<td>7</td>
<td>Respect for user privacy: keep it user-centric</td>
</tr>
</tbody>
</table>
Operationalizing Privacy by Design
Privacy controls framework

- The privacy controls framework is organized around the 7 Privacy by Design principles. Each principle is framed by a set of privacy criteria and illustrative privacy and security controls:

http://ryerson.ca/content/dam/pbdi/Certification/Privacy%20by%20Design%20Certification%20Program%20Assessment_Privacy%20Controls%20Framework%202020150716.pdf

<table>
<thead>
<tr>
<th>Principle</th>
<th>Assessment criteria</th>
<th>Illustrative controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1</td>
<td>1-7</td>
<td>1-18</td>
</tr>
<tr>
<td>Principle 2</td>
<td>8-11</td>
<td>19-32</td>
</tr>
<tr>
<td>Principle 3</td>
<td>12-14</td>
<td>33-38</td>
</tr>
<tr>
<td>Principle 4</td>
<td>15</td>
<td>39-42</td>
</tr>
<tr>
<td>Principle 5</td>
<td>16-24</td>
<td>43-89</td>
</tr>
<tr>
<td>Principle 6</td>
<td>25-26</td>
<td>90-94</td>
</tr>
<tr>
<td>Principle 7</td>
<td>27-30</td>
<td>95-107</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total</th>
<th>30 criteria</th>
<th>107 controls</th>
</tr>
</thead>
</table>

© Deloitte LLP and affiliated entities. | Managing Privacy Risk in the Age of the Internet
Objective and measurable assessment criteria

Our Privacy by Design control framework is based on a set of well-defined privacy criteria and controls that align to the 7 foundational principles:

<table>
<thead>
<tr>
<th>Principle 1: Proactive not reactive; preventative not remedial</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assessment criteria</strong></td>
</tr>
<tr>
<td>1.1 Privacy risk management plan</td>
</tr>
</tbody>
</table>
| A risk assessment strategy and process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and to develop and update responses to such risks. | • A process is in place to periodically assess the organization’s privacy practices, identify the risks to the organization’s personal information and implement mitigating controls.  
  • Such risks may be external (such as loss of information by vendors or failure to comply with regulatory requirements) or internal (such as emailing unprotected sensitive information). When new or changed risks are identified, the privacy risk assessment and the response strategies are updated. The process tracks the implementation of mitigating and corrective actions and re-evaluates practices and risks in a closed loop fashion. |
| 1.1.2 Integration with privacy breach management, complaint resolution and monitoring | • The process considers factors, such as experience with privacy incident management, the complaint and dispute resolution process, and monitoring activities. |
Contextually appropriate data practices

Design choices

Build privacy and security into devices at the outset, rather than as an afterthought – into every stage of development even the design cycle

• Management portals or dashboards
• Icons
• “Out of Band” communications requested by consumers
• General privacy menus
• A user experience approach
• Choices at point of sale
• Tutorials
• Codes on the device
• Choices during set-up
Early adopters

Canadian National Insurance Crime Services

Secure Key

TELUS®

PHEMI Health Systems
Myth #1 Believing that privacy is really the CPO’s problem

- Don’t assume that your project has no privacy implications... And even if it does, don’t assume that the CPO or his or her team will cover off privacy
- Believing there will be no privacy show-stoppers because the CPO is involved is common but potentially risky
- Don’t assume the CPO has a deep understanding of your project
Believing that privacy is really the CPO’s problem
Break the silos

• Everyone working for an organization that depends on personal information is in it together
• Formally document roles, responsibilities and accountability so they are clear:
  – Across departments
    – Define risk ownership
    – Identify and assess interdivisional reliances
    – Formalize data governance
Myth #2 Worrying only about legal compliance

• Privacy is really a legal problem
• Limited or no linkage to business strategy and organizational objectives
• Does not consider risk taking as a means to value creation
• Weak connection to risk appetite
Worrying only about legal compliance
Treat privacy as a strategic business advantage

- Integrate privacy risk management into strategic planning and resource allocation
- Analyze privacy risk and return tradeoff
- Don’t leave privacy as an afterthought – build protections into new technologies upfront
Digital progress
Then and now…

1957:
13 men delivering a computer…

2017:
A person may wear 13 computing devices…
For more information....

Sylvia Kingsmill, BA, LLB
National Partner
Data Protection and Digital Privacy Leader
skingsmill@deloitte.ca
416.643.8238
Deloitte, one of Canada’s leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

The information contained herein is not intended to substitute for competent professional advice.