Privacy Risk Management in a Changing Landscape
Challenges and strategies for decision-makers
by Chantal Bernier

November 18, 2015
Focus

• How is the privacy landscape changing in relation to risk, mitigation strategies and legal context?

• How does it impact decision-makers and how should they manage?
Working assumptions

• Privacy risks are systemic and require system wide risk management plans

• Risks and mitigation strategies are increasingly similar between the private and the public sector – in particular

  • Technological vulnerability crosses sectors
  • New law enforcement powers widen access to both public and private databases
  • Data and data analytics offer value for the public and the private sector— one for governance, the other for profit - and creates legal risks for both
The changing landscape

Technological developments
New risks

• Main vulnerabilities – across sectors:

1. Underestimation or lack of assessment of risk
2. Failure to see privacy risk management as an organizational challenge
3. Insider threat – human error and employee indiscretion

Main vulnerabilities and Best Practices in Data Protection, Canadian Corporate Counsel, volume 24, number 1, December 2014, p.43
New technologies

• Cloud computing: “ubiquitous access to a shared pool of configurable computing resources” \((NIST)\)
  • Risks:
    • Data leakage in multi tenant clouds
    • Loss of control of data through de-localisation
    • Unlawful disclosures for data monetization or to law enforcement
    • Security breaches

• BYOD or “Bring Your Own Device”
  • Risks:
    • Security breaches
    • Compliance monitoring and employee privacy

• Mobile devices
  • Risks
    • Loss of voluminous amounts of information
Mitigation strategies

• Strong governance: OPC recommendations on governance in Google Wi-Fi investigation
  • Employee training
  • Internal compliance mechanisms
  • Assignment of accountability for compliance
  • Accountability of senior personnel
  
  OPC # 2011-001

• Strong implementation: OPC investigation of Employment and Social Development Canada
  • Physical measures to protect devices
  • Technological measures to protect information
  • Administrative measures for risk management

Special Report To Parliament, March 25, 2014
Mitigation strategies continued…

• Personnel security: the example of unauthorized access to health records – OIPC calling for:
  
  • Clear policies to formalize employee privacy obligations
  • Detection mechanisms to prevent and act upon contraventions
  • Regular reminders of employee obligations
  • Appropriate access restrictions
  • Effective breach response strategies including to identify source of breach
  • Disciplinary action to bring policies into effect

OIPC *Detecting and Deterring Unauthorized Access to Personal Health Information* 2015
Mitigation strategies continued…

• Organizational accountability structure:
  • Board of Directors: oversight for proper privacy risk management
  • CEOs: organisational privacy risk management
    • Designating responsible official with effective authority
    • Ensuring the development of relevant policies
    • Overseeing risk assessments
    • Ensuring staff training
    • Adopting breach response plan
    • Verifying compliance
  • CPOs and CIOs: collaboration for a cohesive, integrated approach
  • Line managers: supervision for implementation of privacy policies
  • Staff: compliance with privacy policies

_Five Golden Rules for Accountability on Privacy and Cybersecurity_

Dentons website

November 18, 2015
Mitigation strategies continued...

• On Cloud computing:
  • ISO/IEC 27018 International Code of Practice for PII Protection on the Cloud
  • Comparative Analysis with Canadian Law of ISO/IEC 27018

• BYOD
  • Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization? (https://www.priv.gc.ca/information/pub/gd_byod_201508_e.asp)

• Mobile devices
  • Privacy on the Go: 10 Tips for Individuals on Protecting Personal Information on Mobile Devices (https://www.priv.gc.ca/resource/fs-fi/02_05_d_47_dpd_e.asp)
Changing landscape

Legal developments
New interpretations and provisions

• The principle of openness in the face of overwhelming complexity
• The technological challenges of obtaining valid consent
• New Legislation 2014 – 2015
• European law on data transfers
The principle of openness

• Federal public sector: duty to inform of purpose for collection, *Privacy Act s.5(2)*

• Private sector: duty to
  • Identify purposes (*Principle 4.2, Schedule I PIPEDA*)
  • make available policies and practices (*Principle 4.8, Schedule I PIPEDA*)

• OPC Tips: information that
  • Reflects organization
  • Clearly and succinctly
  • Accessibly
  • With effective privacy controls, and
  • Contact information for queries or complaints
The notion of consent

• Public sector:
  • Collection directly from individual, *Privacy Act s.5(1)*
  • No inconsistent use without consent. *Privacy Act s.7*
  • No disclosure without consent save exceptions, *Privacy Act s.8*

• Private sector
  • No collection, use or disclosure without consent, Principle 4.3, Schedule I, PIPEDA
  • Express or implied is contingent upon sensitivity of information and expectation of privacy, OPC Report of Findings in Bell Canada, Relevant Ads Program, PIPEDA 2015-#001

**Tips:**
• Privacy Impact Assessments to determine valid consent
• Adopt commensurate modalities of seeking consent
New legislation 2014 – 2015

- **Protecting Canadians Online Act**
  - wider law enforcement access powers

- **Security of Canada Information Sharing Act**
  - Information sharing among federal government institutions

- **Digital Privacy Act**
  - Mandatory breach notification
  - Information sharing between organizations
Mandatory breach notification (10.1 PIPEDA)

• Notification of OPC and persons affected
• Where reasonable to believe real or significant harm
• Significant harm is
  • Bodily harm, Humiliation, Damage to reputation of relationships, Loss of employment, business or professional opportunities, Financial loss, Identity theft, Negative effects on credit records, Damage to or loss of property
• As soon as possible

Tips
• Develop policies for criteria and process for notification
• Adopt an anticipated breach response plan
Information sharing among organisations 7(3)d.1,d.2

• Permission to disclose
  • To another organization
  • Where reasonable for the purposes of investigating a breach of agreement, contravention to the law, being or about to be committed, or to deter and detect fraud, and
  • Obtaining consent would compromise the investigation

Tips:
  • Formalize policy on criteria to define “reasonable”
  • Adopt a process to ensure internal compliance
European Union Court of Justice on Safe Harbour

• Invalidation on October 6, 2015

• European companies can only transfer data to the U.S. or via Canada to the U.S. with:
  • Model clauses; or
  • Binding Corporate Rules; or
  • Individual consent

• European Data Protection Authorities require alternatives in place by January 3, 2015
Impact on decision makers

Five game changers and what success looks like
1. Frequency and impact of breaches

- Impact: decision-makers need to demonstrate having made every possible effort

- The picture of success:
  - There is evidence of all available safeguards to safeguards personal information physical, technologically and administratively
  - The measures correspond to risk and to the sensitivity of the information
  - They prove to be effective in resilience to attacks, resisting them or reducing damage
2. Complexity of information management

• Impact: openness is more difficult to achieve and safeguards require a comprehensive risk management framework

• The picture of success:
  • Short, readable and prominent privacy notices on What? Why? and What safeguards?
  • An organizational risk management privacy that links the organisation top to bottom and side to side
The temptation of data

• Impact: unprecedented data volume and analytical capacity call for weighing of collective and private interests in data mining
  • When do you need consent? (OPC on Bell Canada, #2015-001)
  • What is valid consent? (OPC on Bell Canada)
  • How do you ensure compliance? (OPC on Google, #2014-001)

• The picture of success:
  • Privacy Impact Assessment to determine proper course
  • Effective anonymisation (i.e. unlikely re-identification), OR
  • Meaningful information for valid consent
  • Effective compliance monitoring
In short,

• Assess risk according to: what the organization is, what the threats are and the sensitivity of the information

• Adopt corollary mitigation strategies to: ensure valid consent through meaningful notification; provide clear and precise privacy information for openness; safeguard the information with physical, administrative and technological measures

• Make all user relevant information readily accessible with: prominent privacy policy in readable text

• Provide effective choice options: detailed and effective

• Make it an organisational risk management plan that: engages every accountability level and integrates physical, administrative and technological measures into one organisational risk management plan
CASL
2015: review and lessons

Karl Schober
Associate

18 November 2015
This afternoon

1. Spam
   • Investigations
   • Lessons learned
2. Unsolicited Telecommunications
   • Investigations
   • Lessons Learned
3. New computer program installation legislation took effect
Three requirements for CEM

✓ Consent
  • Express
    • Separate
    • A positive action
    • Describe the scope
  • Implied
    • Existing business relationship
    • Existing non-business relationship

✓ Identification
  • Name (individual or organization)
  • Address and phone number, email or website address

✓ Unsubscribe
  • Prominent link or other easy method
  • 10 days to comply
Compu-Finder

- Notice of Violation: $1.1 million administrative monetary penalty
- Period of violation: July 2, 2014 to September 16, 2014
- Allegations:
  - Repeatedly sent CEMs to businesses without consent
  - Unsubscribe mechanisms that did not function properly
Lessons Learned

• B2B?

• Unclear how the CRTC is interpreting two important exceptions:
  • Conspicuous publication
  • Organizations have a relationship and concerns the activities of the recipient of the organization

• Not cooperative?
  • Reading between the lines Compu-Finder may have ignored the CRTC at its peril
Plenty of Fish

• Settlement amount: $48,000
• Period of violation: July 1, 2014 to October 8, 2014
• Allegations:
  • Emails sent to subscribers
  • Notified subscribers of services available
  • Unsubscribe mechanisms not technically compliant, such as:
    • Not “clearly and prominently”
    • Not “readily performed”
• Undertaking
  • Develop a compliance program
Lessons learned

• Communications relating to services may be CEMs or even if they are covered by section 6(6) (i.e. no consent required for factual information about a subscription) they require an unsubscribe

• Ensure “unsubscribe” mechanism is clearly and prominently labelled

• Settling quickly may be rewarded
Porter Airlines

• Settlement amount: $150,000
• Period of violation: July 1, 2014 to February 23, 2015
• Allegations: Sent CEMs without an unsubscribe mechanism, or the unsubscribe mechanism did not comply with CASL, such as:
  • Not “clearly and prominently”
  • Lack of complete contact information
• Unable to prove consent
• Undertaking
  • Update and implement its compliance program
Lessons Learned

• Records Matter
  • Need to be able to prove consent or exception to consent

• CEM Content Matters
  • Identification information needs to be complete
    • Clearly identify name, address and phone number, email or website address

• Review your unsubscribe mechanism and ensure all methods function properly

• Users who continue to receive CEMs after unsubscribe fails will complain

• Accountable for third parties sending CEMs on your behalf
Unsolicited telecommunications

1. Consumers register their numbers with the National DNCL

2. Telemarketers
   • To sell or promote a product or service, or to request donations
     • Exempt where they have an existing business relationship
     • Exempt also includes registered charities, newspapers, political parties, market research and survey organizations
     • Registration and subscription

3. Rules
   • Identification
   • Display
   • Time period
   • Adhere to National DNC list
   • Internal DNC list

4. ADAD

5. Record keeping
Unsolicited telecommunications investigations

- Hamel Systeme d’Information 2000 Inc. (Telelisting)
  - Allegations: Reselling access to the DNC List to real estate agents
  - Fine of $260,000
- Metroland
  - Allegations: Automatic dialing-announcing device sending non-compliant messages
  - Fine of $240,000
- Rainmaker Marketing/Maple Accounting
  - Allegations: U.S. company not registered or subscribed to the National DNCL. Calling Canadians without consent.
  - Fine of $145,000
- Caribbean Cruise Line Inc.
  - Allegations: U.S. company calling Canadians registered on the DNC
  - No valid exemption
  - Fine of $200,000
Installing computer programs legislation takes effect

Consent is required to install or cause the installation of a computer program (software) to another person’s device in the course of a commercial activity.

• **Why care?**
  • Fines of up to $10,000,000 for organizations and $1,000,000 for individuals
  • Upcoming right of private action

• **All computer programs?**
  • Deemed consent
    • Cookies, Java, solely for security purposes

• **Consent must include:**
  • The purpose (to install)
  • Identify the installer (or on whose behalf)
  • Mailing address and one other piece of contact info
  • Notify the individual they can withdraw
  • Description of the functions and purpose of the program
Installing computer programs legislation takes effect

• Enhanced disclosure and consent requirements:
  • Collects personal information
  • Interferes with user’s control
  • Changes or interferes with data stored
  • Causes the computer system to connect or send messages to other computers systems
  • Installs a program that may be unknowingly activated by a third party, etc.

…if contrary to the reasonable expectations of the owner or authorized user.

Withdrawal of consent based on inaccurate description program’s material elements?

• What about consent for upgrades or updates?
  • How do you get consent pre-installed by the owner?
  • How do you get consent from purchasers who buy a used good? Does consent transfer?

• January 15, 2018: Three year transition period
• Keep records

18 November 2015
Thank you

Dentons Canada LLP
77 King Street West
Suite 400
Toronto, Ontario M5K 0A1
Canada

Dentons is the world's first polycentric global law firm. A top 20 firm on the Acritas 2015 Global Elite Brand Index, the Firm is committed to challenging the status quo in delivering consistent and uncompromising quality and value in new and inventive ways. Driven to provide clients a competitive edge, and connected to the communities where its clients want to do business, Dentons knows that understanding local cultures is crucial to successfully completing a deal, resolving a dispute or solving a business challenge. Now the world's largest law firm, Dentons' global team builds agile, tailored solutions to meet the local, national and global needs of private and public clients of any size in more than 125 locations serving 50-plus countries.