Bennett Jones

ACC Association of Corporate Counsel
ONTARIO

The Changing Landscape of Privacy Regulation in Canada

Ruth Promislow,
Partner, Bennett Jones

Cailey Greenberg,
Senior Counsel, Global Privacy and Compliance, Canopy Growth

June 2, 2021

TODAY'S TOPICS

- Proposed changes in privacy legislation
- Critical issues for corporate counsel to address

PROPOSED CHANGES TO PRIVACY LEGISLATION

- Status – draft federal privacy legislation:
  - Introduced November 2020
  - Federal Privacy Commissioner has called the draft "a step back for privacy"

- 3 key aspects of draft legislation
  - Enhanced compliance obligations
  - Penalties and private right of action
  - Privacy Commissioner powers

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

Enhanced Compliance Obligations

1. Privacy management program
    - Policies, practices and procedures put in place to fulfill obligations

2. Spot Check
    - Must provide access to privacy management program
    - Privacy Commissioner cannot use what he learns to initiate complaint or audit
    - *Privacy Commissioner comments:*
        - He wants to be able to initiate complaint or audit without basis for believing there is contravention; 'look under the hood'

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

Enhanced Compliance Obligations

3. Identify and document purposes
    - Limit use to those purposes; penalty for use beyond
    - Delete upon request
    - *Privacy Commissioner comments:*
        - *specific, explicit and legitimate purposes should be required*
        - *Wants to avoid use of identified purposes such as "improving your customer experience"*

4. Appropriate purpose analysis
    - Prescribed factors to consider, includes balance between impairment of rights and business needs
    - *Privacy Commissioner comments:*
        - *Analysis should go beyond 'appropriate purpose' and consider whether appropriate means used to collect information*
        - *Privacy rights to be recognized as quasi-constitutional right*

Bennett Jones

ACC Association of Corporate Counsel ONTARIO

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

Enhanced Compliance Obligations

5. Requirements for Consent

- Prescribed information to be disclosed:
  - purposes; way in which information collected/used/disclosed; reasonably foreseeable consequences; types of PI; third parties
- Business activity exemptions
  - For business activity listed (e.g. provide product requested)
  - Reasonable purpose would expect collection
  - No collected/used for purpose of influencing behavior/decision

- *Privacy Commissioner position:*
  - Exemptions overly broad
  - need requirement that individual understands nature, purpose and consequence of consenting

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

Enhanced Compliance Obligations

6. Trans-border data flows
    - No specific changes
    - *Privacy Commissioner comments:*
        - Need additional provisions to address:
            - » Who is accountable for the personal data that flows across borders and in what circumstances? Need to account for data flow that is not simply transfer to service provider
            - » What conditions must be met before the personal data can flow across borders?
                - May include notice to individuals, level of protection required, or the safeguards and contractual or other measures that must be in place

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

Enhanced Compliance Obligations

7. Transparency – must make readily available:
    - Description of PI
    - How org makes use of PI
    - Use of any automated decision system to make predictions, recommendations or decisions
    - International or interprovincial transfer/disclosure that may have implications
    - How individual can make request for disposal of PI

8. Algorithmic transparency
    - Must, on request, provide individual with:
        - explanation of the prediction, recommendation or decision and of how PI that was used to make the prediction, recommendation or decision was obtained

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

Enhanced Compliance Obligations

9. Security safeguards
    - Physical, organization and technological safeguards
    - Level of protection must be proportionate to sensitivity of information
    - **New:** must consider quantity, distribution, format and method of storage

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

Penalties

- Privacy Commissioner can recommend to Tribunal that penalty be imposed
- Penalties for non-compliance with obligations ($10M/3% gross global revenue)
  - Limit collection/use/disclosure to recorded purposes
  - Deceptive or misleading practices.
  - Limit retention
  - Dispose of information upon request
  - Safeguard information
  - Report data breach involving real risk of significant harm

- *Privacy Commissioner comments:*
  - List needs to be longer and include failure to obtain valid/meaningful consent
  - He should be able to impose penalties; rather than recommend

Bennett Jones

ACC Association of Corporate Counsel ONTARIO

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

Penalties for knowing contravention ($25M/5% gross global revenue)

- Failure to report breach
- Failure to keep record of every breach of security safeguards
- If request regarding automated decision making, retain information so individual can exhaust recourse
- Must not use de-identified information to identify an individual
- Penalty imposed on employee who reports contravention of obligations
- Failure to comply with order by Privacy Commissioner
- Obstruct Commissioner in investigation of complaint [e.g destruction of records]

Bennett Jones

ACC Association of Corporate Counsel ONTARIO

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

- Commissioner may order organization to:
  - Take measures to comply with the Act
  - Stop doing something that is in contravention of the Act
  - Comply with terms of compliance agreement
  - Make public measures taken to correct policies, practices or
  - procedures of organization
- Commissioner may recommend penalty to tribunal

- *Privacy Commissioner comments:*
  - *Privacy Commissioner should be empowered to impose penalty directly*

Bennett Jones

ACC Association of Corporate Counsel ONTARIO

PROPOSED CHANGES TO PRIVACY LEGISLATION (cont'd)

Private right of action

- Individual who is affected by act or omission that constitutes contravention has cause of action against org for damages for loss or injury.
- *Class action risk*
- *Lower burden of proof vs invasion of privacy claim*
  - *Invasion of privacy claim requires evidence of intentional/reckless conduct*
  - *Contravention of statutory obligations – no evidence of intent required*

Bennett Jones

ACC Association of Corporate Counsel ONTARIO

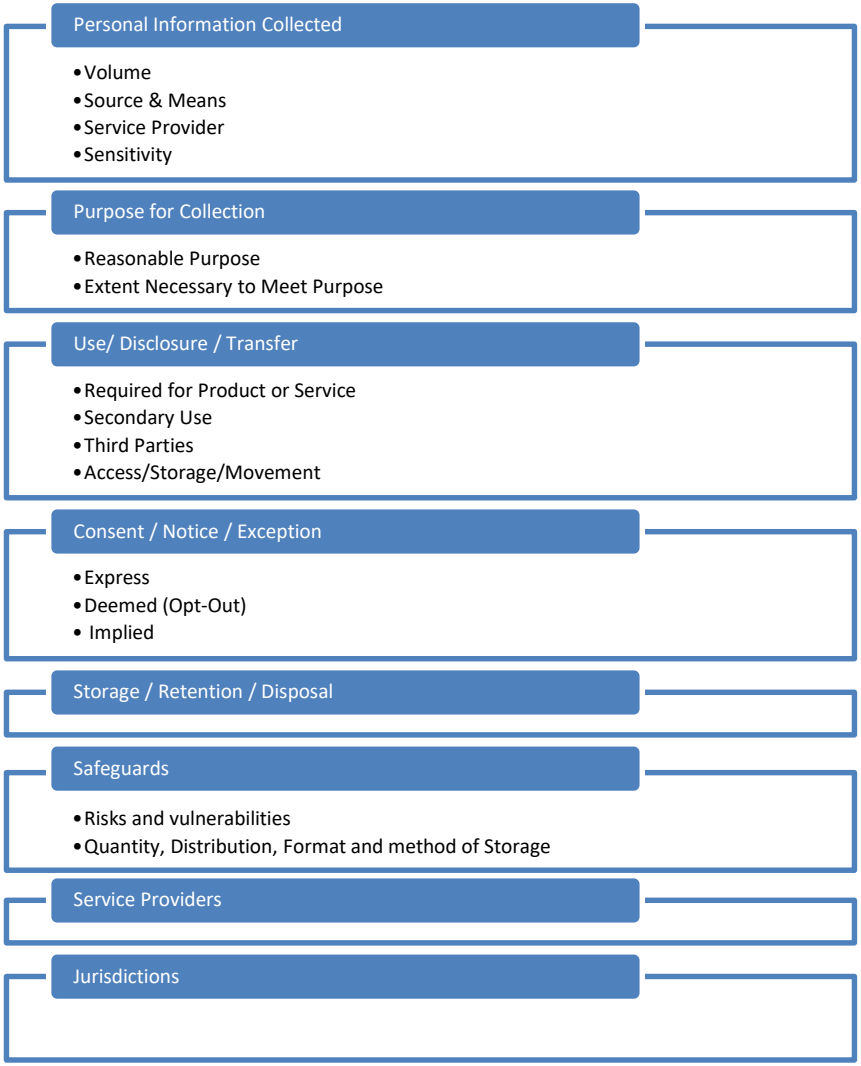
KEY ISSUES FOR CORPORATE COUNSEL TO ADDRESS

1. Data mapping
2. Risk & Vulnerability Review
3. Risk Management Framework
4. Policy Development

Bennett Jones

ACC Association of Corporate Counsel ONTARIO

DATA MAPPING



Bennett Jones

ACC Association of Corporate Counsel ONTARIO

RISK & VULNERABILITY REVIEW

- Assess and document risks and vulnerabilities to your operations
- Examples of risks include:
  - External attacker; third party supplier breach; hostile insider; employee error (e.g. click on malicious link); use/disclosure beyond permitted consent

- Examples of vulnerabilities include:
  - Network
    - How easily can intruder hack into network
    - How easily can you detect presence of intruder
    - Do third party service providers have access to your network

- Operations
  - Lack of employee training
  - Remote access without multifactor authentication
  - No one responsible for patching software
  - Sensitive information can be downloaded to laptops and circulate via email
  - Sensitive documents stored in unlocked filing cabinet
- Develop framework for managing risks

Bennett Jones

ACC Association of Corporate Counsel ONTARIO

RISK MANGEMENT FRAMEWORK

- Establish roadmap for managing risks
- Outsourcing
- **Risk:** If third party provider which process personal information we collect is attacked, may have exposure.
- **Risk Management:**
  - Vet provider for security and document that process;
  - Understand how vendor operates (subcontractors? Process/store information in other jurisdictions);
  - Impose contractual terms;
  - Establish audit protocol

RISK MANAGEMENT FRAMEWORK (cont'd)

- Collect highly sensitive information (SIN; Driver's License)
- **Risks:** hostile outsider attack; careless employee; hostile employee
- **Risk Management:**
  - Segregate highly sensitive data
  - Limit access on need to know basis
  - Log access
  - Limit ability to download information
  - If data has to be transferred, it must be encrypted
  - Multi-factor authentication

RISK MANAGEMENT FRAMEWORK (cont'd)

- Ransomware Attack
- **Risk:** employee can download malware by clicking on malicious link
- **Risk Management:**
  - Regularly update system with appropriate security patches
  - Filter web and email content for malicious URLs
  - Use multi-factor authentication on all accounts
  - Implement least privilege
  - Back-up strategy
  - Employee training – regular training and reminders
  - Monitor supply chain security, including software/hardware suppliers
  - Incident response plan – rehearse code-red scenarios

RISK MANAGEMENT FRAMEWORK (cont'd)

- Data Breach
- **Risk:** Collect large amounts of personal information and exposure if you are breached
- **Risk Management:**
  - Map data so you know full extent of all categories of information collected
  - Rank categories of information based on sensitivity
  - Limit how data moves around internally and externally
  - Consider segregating highly sensitive information; limit access
  - Implement data retention policy so that personal information is disposed of when no longer required
  - Multi-factor authentication
  - Strong password policy (regular forced password changes and require complex passwords)
  - Filter web and email content for malicious URLs

RISK MANAGEMENT FRAMEWORK (cont'd)

- Privacy violations
- **Risk:** Collect/use/disclose information without consent; fail to dispose of information when no longer required; fail to implement required safeguards; fail to be transparent re: personal information practices
- **Risk Management:**
  - Data mapping
  - Identify risks and vulnerabilities
  - Develop risk management framework
  - Develop policies

POLICY DEVELOPMENT

Defensive Documentation

- Data mapping
- Privacy policies (internal/external/employee)
- Incident response plan
- Information technology
- Automated decision making
- Outsourcing
- Security Policy (technological; operational; physical)
- Transparency documentation
- Complaints/Inquiries
- Employee training (security threats; and corporate privacy program)
- Audit Cycle

Bennett Jones

ACC Association of Corporate Counsel ONTARIO

Q&A

- QUESTIONS?

THANK YOU!

Ruth Promislow

416 777 4688

promislowr@bennettjones.com

Bennett Jones

ACC Association of Corporate Counsel ONTARIO