The Digital Privacy Act, and Other Privacy Updates

Presented by:

Wendy Mee

BUSINESSCLASS
KNOWLEDGE ▪ SEMINARS ▪ INSIGHTS

Blakes

Privacy Sector Privacy Laws

- *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**")
- Quebec's *Act respecting the protection of personal information in the private sector*
- Alberta *Personal Information Protection Act*
- British Columbia *Personal Information Protection Act*
- *Canada's Anti-Spam Legislation*

Fair Information Handling Principles

- 10 basic principles that underlie all privacy legislation in Canada
- Based on the CSA Model Code for the Protection of Personal Information

10 Fair Information Handling Principles

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

10 Fair Information Handling Principles

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

Accountability

- An organization is responsible for PI under its control including PI transferred to a service provider for processing
- Must designate and identify an individual(s) to be accountable for the organization's compliance with FIPs (e.g. Privacy Officer)
- Must implement policies and practices to give effect to FIPs

Consent

- Collection, use and disclosure of PI must be with consent, unless exemption applies.
- Consent can be express, implied or negative option (express consent generally required for sensitive PI like health and financial information).
- Consent must be informed.
- Consent to “secondary” use of PI must not be mandatory.

Limiting Collection

- Collection of PI must be limited to what is necessary for the identified purpose.
- Additional PI can be requested but cannot be mandatory.

Limiting Retention

- Personal information may be retained only as long as necessary to fulfill the purposes for which it was collected.
- Record retention policies and procedures should be developed, with minimum and maximum retention periods.
- Personal information that is no longer required should be destroyed, erased, or made anonymous.

Safeguards

- PI shall be protected by security safeguards (physical, organizational, technological) appropriate to the sensitivity of the information, throughout lifecycle
- The nature of the safeguards will vary depending on the sensitivity of the PI, amount of PI, storage medium, etc.
- Employees must be made aware of the importance of privacy and security of PI

Reasonableness

- An organization can only collect, use and disclose personal information for purposes that a reasonable person would consider are appropriate in the circumstances.

Digital Privacy Act

Key amendments to PIPEDA:

- Explicit requirements for valid consent
- Updated definition of personal information (PI)
- New exemptions from consent requirement
- New power for OPC to enter into compliance agreements
- Mandatory breach notification provisions (not yet in force)

Digital Privacy Act *(cont'd)*

- An individual's consent is only valid if it is reasonable to expect that the individual would understand the nature, purpose and consequences of the collection, use or disclosure of the PI to which he/she is consenting

Digital Privacy Act *(cont'd)*

- Business contact information more broadly defined but no longer excluded from definition of PI
- However, PIPEDA Part I not applicable to collection, use or disclosure of business contact information solely for the purpose of communicating with an individual about his/her employment, business or profession
- Similar provision under Alberta PIPA
- B.C. PIPA exempts business contact information from PI
- But don't forget Quebec and CASL!

Digital Privacy Act (cont'd)

Several new exceptions from PIPEDA's consent requirement, including:

- In connection with a business transaction
- For PI produced in the course of employment, business or profession ("work product exception")
- In connection with investigating breach of an agreement, contravention of law, detecting, suppressing or preventing fraud or insurance claims

In each case, <u>provided certain conditions are met</u>

Digital Privacy Act *(cont'd)*

- Commissioner can enter into compliance agreement where he has reasonable grounds to believe that an organization has committed, is about to commit or is likely to commit a breach of PIPEDA
- May contain any terms necessary to ensure compliance
- Failure to abide by compliance agreement allows Commissioner to apply to the Federal Court for remedies, including an order requiring compliance

Digital Privacy Act *(cont'd)*

- Mandatory breach notification (not yet in force)
- Affected individuals and Commissioner must be notified where breach poses "real risk of significant harm"
- Government institutions/other organizations must be notified in prescribed circumstances
- Must maintain records of all data breaches, including those that do not meet harm threshold, and report to Commissioner upon request
- Failure to report/record an offence punishable by fines of up to C$100,000

Questions?

wendy.mee@blakes.com