CORPORATE COMMUNICATION: Confidentiality, Privacy and Privilege

*Best Practices in Privacy Policy Development, Enforcement & Review*

*and*

*Privacy Considerations in Business Transactions*

Brian Thiessen
Partner
Blake, Cassels & Graydon LLP
Best Practices in Privacy Policy Development, Enforcement & Review

The Importance of Privacy Polices & Practices
• The Value of a Proactive Approach

• Negative Consequences of Non-Compliance:
• a) Proceedings before the Privacy Commissioner
• b) Being found guilty of offences under PIPA
• c) Civil liability pursuant to s. 60 of PIPA.

• Jones v. Tsige, 2012 ONCA 32: Ontario Court of Appeal awards damages on basis of the tort of “intrusion upon seclusion.”
Best Practices in Privacy Policy Development, Enforcement & Review

Privacy Policy Development – Key Questions:

• What types of information does your organization collect from individuals? How? Third parties involved?
• What information does your organization use? How?
• What information does your organization disclose or transfer to third parties? How? Is information transferred outside Canada? Third parties involved?
• How is personal information stored? Destroyed? What security measures are employed?
• Who should serve as Privacy Officer?
Best Practices in Privacy Policy Development, Enforcement & Review

POLICY NOTE: Document Retention

• Consider how document retention requirements impact your privacy policies regarding document storage and destruction.

POLICY NOTE: International Service Providers

• If your organization uses service providers outside Canada to collect, use, disclose or store personal information, must include in your privacy policy:
  – Purpose for which the service provider has been authorized to collect/use/disclose the information.
  – Countries outside Canada in which collection/use/disclosure is occurring or may occur.
• Notification Requirement
Best Practices in Privacy Policy Development, Enforcement & Review

Policies are in place – now what?

- **Communicate** your policy to affected individuals (customers, employees, service providers, etc.).

- Establish an effective **complaint handling process**. Process should be: accessible, understandable, easy to use, fair, impartial and confidential.

- **Enforce the policy**: When issues occur, investigate and take appropriate measures to rectify the situation including correcting information handling practices, communication those changes to relevant staff, and informing complainant of steps taken.
Best Practices in Privacy Policy Development, Enforcement & Review

Ensuring Continuing Compliance - Privacy Audits:

- As your organization grows and changes and the law in this area develops, your organization’s privacy policies and practices should be reviewed and updated – a great way to do this is a privacy audit.

- **Privacy Audit – 3 Steps:**
  - Taking an inventory of your personal information holdings
  - Identifying the information needs of the different functions within your organization
  - Identifying your current information practices.

Blakes
Privacy Considerations in Business Transactions

Quote from the Builder’s Investigation Report:

[…] law firms have shown a lack of attention to the impact of privacy laws on the myriad legal processes involving the collection, use and disclosure of personal information, including client information and third party information that are common in the type of work they perform on behalf of their clients. Privacy laws are complex, and have implications for their clients on many different types of transactions, including mergers and acquisitions such as in the present case. We believe that lawyers and law firms require heightened awareness and knowledge of privacy laws in order to properly recognize these implications.
Privacy Considerations in Business Transactions

Consider: Is the transaction regulated? By?

• Federal (PIPEDA)
  – Applies to: Federal works and undertakings and businesses/personal information that is collected/used/disclosed inter-provincially or internationally or in provinces without privacy legislation.

• Provincial (PIPA in BC, Alberta, Quebec)
  – Applies to: Businesses/personal information where provinces have enacted privacy legislation and not a federal work or undertaking.

• Cross Border Transactions (PIPEDA+)
  – Interprovincial and international borders subject to PIPEDA
  – Example: Sale of an inter-provincial pipeline.
  – Provincial and federal legislation can be applied in tandem.
Privacy Considerations in Business Transactions

Alberta’s *Personal Information Protection Act*

- Specific “Business Transactions” exception.
- Builder’s Investigation Report
  - **Personal Information that may be necessary to complete a business transaction:** Names and titles of employees, descriptions of positions and functions, descriptions of an individual’s place in the acquired organizations management structure, salary levels (in some cases) and outstanding employee litigation (in some cases).
  - **Business transaction exception does not apply to employees’ home addresses or Social Insurance Numbers.**
Privacy Considerations in Business Transactions

- Considerations for Confidentiality Agreements:
  - A definition of Personal Information
  - A declaration that the use and disclosure of information is restricted to those purposes that relate to the particular business transaction.
  - A declaration that the information is necessary for the parties to determine whether to proceed with the business transaction.
  - An undertaking from the Purchaser after closing of the transaction, to use and disclose the information only for those purposes for which the information was initially collected from or in respect of the individuals.
Privacy Considerations in Business Transactions

• Considerations for Confidentiality Agreements (cont’d):
  – A declaration that the information relates solely to the carrying on of the business or activity or the carrying out of the objects for which the business transaction took place.
  – A declaration that, in the event the business transaction does not proceed or is not completed, the party to whom the personal information was disclosed must, if the information is still in the custody of or under the control of that party, either destroy the information or turn it over to the party that disclosed the information.
Privacy Considerations in Business Transactions

BC’s *Personal Information Protection Act*

- BC PIPA requires that individuals whose personal information has been disclosed as part of a business transaction be notified that the transaction has occurred and their personal information has been disclosed after the transaction (Section 20(3)(c)).

Blakes
Privacy Considerations in Business Transactions

**Federal PIPEDA**

- No business transaction exception currently in force.
- Amendments proposed to create disclosure exception for personal information for prospective/completed business transactions.
- Until Bill C-12 is passed:
  - Try to maintain confidentiality of employee information by anonymizing information.
  - Any consent must expressly state that the employee consents to disclosure for the purpose of a merger or acquisition.
Privacy Considerations in Business Transactions

Cross Border Transactions

- U.S “safe harbour” approach has created concern regarding sharing personal information with U.S. entities
- Federal Privacy Commissioner has stated:
  - *PIPEDA* contains an accountability principal that imposes responsibility on an organization for information that has been transferred to a third party for processing. Clause 4.1.3 of the Schedule 2 *PIPEDA* requires the organization to use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. This principal applies to any transfer, whether the receiving company is in Canada or abroad.
- U.S. entity will have to ensure it enacts similar privacy protection policies to the Canadian entity to ensure compliance.
Privacy Considerations in Business Transactions

Potential Future Change to US Privacy Law

• White House Report (February 24, 2012) calls on Congress to codify the Consumer Privacy Bill of Rights. This new federal law should:
  – Allow the FTC and state Attorneys General to enforce the law directly (there is no mention of a private right of action).
  – Pre-empt state privacy laws that are inconsistent with the Consumer Privacy Bill of Rights.
  – Avoid prescribing technology-specific means of complying with the law's obligations.
  – State companies' obligations under the Consumer Privacy Bill of Rights with greater specificity than the Bill of Rights provides.
  – Establish a safe harbor from enforcement for companies that adhere to voluntary codes of conduct that the FTC has reviewed and adopted.
  – Set a national standard for security breach notification.
Privacy Question? Calgary Privacy Group at Blake, Cassels & Graydon LLP

Brian Thiessen
(403) 260-9616

Maxwell Brunette
(403) 260-9701

Claire Marchant
(403) 260-9641

Krista Schofer
(403) 260-9774