New Privacy Legislation: What it means to law firms

Nova Scotia Barristers' Society

13 November 2003

David T.S. Fraser
David.fraser@mcinnescooper.com
(902) 424-1347

Canadian Privacy Law

Introduction to the
Personal Information Protection and Electronic Documents Act

Agenda

- What is meant by “privacy”
- History of privacy laws
- Personal Information Protection and Electronic Documents Act
  - Constitutional issues
  - Phased-in implementation
  - What is meant by “personal information”
  - The ten principles
  - Does it apply to your firm?
  - What about employees?
- Quirks for law firms
- Exceptions for (almost) every rule
  - Consent
  - Access
- Action plan

Privacy – What are we talking about?

- Has been characterised as the right to be left alone, to be secure in one's home and free from unwanted interference
  - Trespass, nuisance, developing tort of invasion of privacy
- In the context of the new law, privacy means having control over one's personal information
    - Choice of whether to disclose information at all
    - Control over with whom it is shared
    - Control over how it is used
    - Don't lose control once you've released your information "into the wild"

History of Privacy Laws

- Public sector laws dated back 20+ years
  - *Privacy Act* – protection of personal information held by federal government
  - *Freedom of Information and Protection of Privacy Act* (NS) – protection of personal information held by the provincial governments
- No private sector laws until recently
  - Only Quebec (1994)!
- According to surveys, one significant impediment to widespread adoption of electronic commerce has been consumer privacy.
- Part of the federal government's e-commerce agenda, but not limited to online activities

Privacy - PIPEDA

- PIPEDA is implemented in a unique way that demonstrates its unusual constitutional position.
  - Property and civil rights in a province generally recognized to be **provincial** jurisdiction.
  - Privacy is a civil right ∴ provincial jurisdiction (?!)
  - But commerce is inter-provincial, international, inter-jurisdictional.
  - Federal government is relying on the general trade an commerce powers.
  - Some constitutional scholars say it is unconstitutional.
  - Government decided on a phased-in implementation to allow provinces to enter the field and to avoid a constitutional argument with Quebec.

Privacy - PIPEDA

- Phased in application
  - 1 January 2001 - Federal Private Sector
    - Telecommunications, railways, air travel, shipping, credit bureaus, banks
  - 1 January 2004 - Provincial Private Sector
    - The rest of the economy
    - Lawyers, law firms, etc.
- Exemption if provincial government steps in and passes legislation that is declared to be "substantially similar".

No such legislation in Atlantic Canada – none anticipated

Privacy - PIPEDA

- Exclusions
  - Areas already covered by federal *Privacy Act*.
  - Domestic purposes – personal address book, Christmas card list
  - Information compiled for journalistic, artistic or literary purposes

Privacy - PIPEDA

- Addresses "personal information" – information about an identifiable individual:
  - **NOT** name, title, business address or telephone number of an employee or organization
  - Would include name, address, income, health information, demographics, preferences, birth date, SIN, customer numbers, unique identifiers
  - Also includes analysis or opinions about an individual
- Also includes information that may be traced back to an individual

Privacy Principles

- Based on the principles of the Canadian Standards Association Model Code for the Protection of Personal Information:

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

Principles

1. **Accountability** - an organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the principles contained in the Canadian Standards Association model code for the protection of personal information.
2. **Identifying Purposes** - the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent** - the knowledge and consent of the individual are required for the collection, or disclosure of personal information, except where inappropriate. Form of consent is dependent upon the sensitivity of the information

Principles

4. **Limiting Collection** - the collection of personal information shall be limited by that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention** - Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Principles

6. **Accuracy** - Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards** - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness** - An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principles

9. **Individual Access** - Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance** - An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Does it apply to law firms?

- *Yes.*
- *PIPEDA*, s. 4(1):

  "… applies to every organization in respect of personal information that

  (a) the organization collects, uses or discloses in the course of commercial activities; or

  (b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."

- Practice of law may be a profession, but it is "commercial activity" for the purpose of the Act.

Does it apply to you?

- "… in the course of commercial activities… "
  - Defined in the Act to mean:

    "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund raising list"
  - Subject is the "**transaction, act or conduct**", not the whole enterprise
  - You can be non-profit, but engage in some commercial activities under the Act
    - universities operating bookstores, health clubs, etc.
    - university alumni offices selling names to "affinity" providers.

What about employees?

- PIPEDA only applies generally to employee information in the federally-regulated private sector
- Law firms are provincially regulated, so PIPEDA does not apply to your employee information.
- Employee information is only covered in the provincially-regulated private sector if it is used in a commercial way

Consequences

- Individual (not just client!) can make a written complaint to the Privacy Commissioner (s. 11).
  - Commissioner may initiate a complaint of his own accord.
  - Commissioner investigates the complaint
  - Powers in s. 12(1): Compel evidence, administer oaths, accept any evidence whether ordinarily admissible (or not), **enter any premises** other than a dwelling, review documents, etc.
- Commissioner's Report
  - To contain findings and recommendations, whether there was a settlement
  - Commissioner can decline to issue a report if the complainant has other recourse available

Consequences

- Court hearing
  - A complainant (***not the organization***), after receiving the Commissioner's report, may apply to the Federal Court – Trial Division for a hearing.
- Court's remedies include:
  - Order the organization to correct its practices in order to comply with ss. 5-10 of the Act;
  - Order the organization to publish a notice of actions taken to correct its practices; and
  - Award damages, including damages for humiliation the complainant may have suffered.

Consequences for lawyers

- Unclear whether professional regulators will consider non-compliance with PIPEDA to be professional misconduct.

Quirks for Lawyers

- Need to be aware of for whom you are collecting, using or disclosing personal information: for you or for your client?
- If for client:
  - Probably acting as agent's client
  - Can do what the client would be able to do him/her/itself.
  - Need to make sure that the client has the requisite consent to collect, use or disclose personal information in question or make sure an exception applies.

Quirks for Lawyers

- If for yourself or your firm:
  - Need to comply yourself
  - Ask if it really is “personal information”
    - mailing list of bank managers (with work addresses) is not “personal information”
    - Marketing to individuals is much more problematic
  - If it is personal information, you need to comply yourself

Quirks for Lawyers

- Public registry information – PPSA, real property, bankruptcy, court registry, etc.
- No longer "fair game"
- S. 7(1)(d) says you can use personal information without consent if it is "publicly available" and is specified in the regulations
- **But**!
- Regulations specify:
  - (*c*) personal information that appears in a **registry collected under a statutory authority** and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry;
  - (*d*) personal information that appears in a **record or document of a judicial or quasi-judicial body**, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document; and

- Can't use it as a general investigative tool.

Quirks for Lawyers

- This law can actually help lawyers and their clients! (surprise!)
- Pre-litigation discovery tool:
  - Everyone has a right of access to their personal information
  - Just need to ask for it

Consent Exceptions

- Section 7 of PIPEDA sets out the allowed exceptions to the general consent rule
- **Warning**:
  - Not very easy to follow.
  - May not allow you to do what you want.
  - Adult supervision required!
- Some exceptions that are specific to law firms

Consent Exceptions – s. 7

- S. 7(1) – Allows some collection
- S. 7(2) – Allows some use
- S. 7(3) – Allows some disclosure

- Be careful that allowed collection may not lead to allowed use → at least not according to the statute.

Consent Exceptions

- Consent exceptions are very dangerous
- Virtually all circumstances are fraught with risk:
  - Clearly in interests of individual and consent cannot be obtained in a timely way.
  - Investigation
  - Journalistic or artistic purposes / scholarly purposes
  - Publicly available information
  - Emergency
  - To a lawyer
  - Collecting a debt
  - Subpoena
  - To government institution for national security, defense of Canada, etc.
  - Investigative body, government institution
- Permissive exceptions, not mandatory
  - S. 7 allows you to do things that would otherwise be unlawful under PIPEDA … does not force you to do so.

Consent Exceptions

- S. 7(1)(a) & 7(2)(b) – "If clearly in the interests of the individual and consent cannot be obtained in a timely way."
  - Can be collected and used
  - No decisions yet.

Consent Exceptions

- S. 7(1)(b) – "it is reasonable to expect that the collection with the knowledge or consent of the individual **would compromise** the availability or the accuracy of the information and the collection is reasonable for purposes **related to investigating a breach of an agreement or a contravention of the laws of Canada or a province**."
  - Can be collected and used
  - Has been used and upheld by bank in the course of fraud investigation
  - Probably applies to investigating insurance fraud
  - But is a tort a "contravention of the laws of … a province?"

Consent Exceptions

- S. 7(1)(c) – "the collection is solely for journalistic, artistic or literary purposes; …"
  - Allows collection
  - No decisions

Consent Exceptions

- S. 7(1)(d) – "the information is publicly available and is specified by the regulations"
- Regulations specify:
  - (*a*) personal information consisting of the name, address and telephone number of a subscriber that appears in a **telephone directory that is available to the public**, where the subscriber can refuse to have the personal information appear in the directory;
  - (*b*) personal information including the name, title, address and telephone number of an individual that appears in a **professional or business directory**, listing or notice, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the directory, listing or notice;
  - (*c*) personal information that appears in a **registry collected under a statutory authority** and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry;
  - (*d*) personal information that appears in a **record or document of a judicial or quasi-judicial body**, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document; and
  - (*e*) personal information that appears in a **publication**, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information.
- Just because it is publicly available doesn't mean it is "fair game". Most can only be used for consistent purposes.

Consent Exceptions

- S. 7(2)(b) – "it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;"
  - Doesn't have to be that individual's life, health or security at stake
  - Use exception
- S. 7(3)(e) – "(*e*) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;"
  - Disclosure exception

Consent Exceptions

- S. 7(3)(c) – "may disclose information … if required to comply with a **subpoena** or **warrant** issued or an **order made by a court, person or body with jurisdiction to compel the production of information**, or to **comply with rules of court** relating to the production of records"
  - Allows **disclosure**
  - **Permissive, not mandatory** – PIPEDA says you can disclose, but does not say you must
  - Clients need to be careful not to accidentally waive privilege

Consent Exceptions

- S. 7(3)(c.1) – "made to a government institution or part of a government institution that has made a request for the information, **identified its lawful authority** to obtain the information and indicated that
  - (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
  - (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
  - (iii) the disclosure is requested for the purpose of administering any law of Canada or a province."
  - Allows **disclosure**
  - Be very careful with this exception
  - **Permissive, not mandatory** – should not interfere with privilege.
  - Note that the government body needs to have lawful authority to obtain the information and they have to request it.

Consent Exceptions

- S. 7(3)(*d*) – "made on the initiative of the organization to an **investigative body**, a **government institution** or a part of a government institution and the organization
  (i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
  (ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;"
  - Allows **disclosure**
  - Made on the initiative of the organization
  - "Investigative body" is defined in the regulations:
  - Presently only
    - the Insurance Crime Prevention Bureau, a division of the Insurance Council of Canada; and
    - the Bank Crime Prevention and Investigation Office of the Canadian Bankers Association.
  - Bar society may become an investigative body.

Consent Exceptions

- Miscellaneous **disclosure** exceptions
  - 7(3)(g) – archival institution for the purposes of conservation
  - 7(3)(h) – after the earlier of (a) 100 years after the creation of the record or (b) 20 years after the death of the data subject.
  - 7(3)(h.2) – made by an investigative body for reasonable purposes related to investigation of breach of an agreement or the laws of Canada or a province
  - 7(3)(i) – required by law

Access Exceptions

- S. 9 contains exceptions to the general right of access
- Again, must be very carefully exercised

Access Exceptions

- 9(1) - **Prohibited** from providing access if it would reveal third-party personal information, but if you can sever the third-party information you must do so.
  - 9(2) – (1) does not apply if the third-party consents to the disclosure or if it is needed because an individual's life, health or security is threatened.

Solicitor Client Privilege

- Exception to the Access Principle:
- When access may be refused (permissive)

9(3) "Despite the note that accompanies clause 4.9 of Schedule 1, an organization is not required to give access to personal information only if

(*a*) the information is protected by **solicitor-client privilege**;

....

(4) Subsection (3) does not apply if the individual needs the information because an individual's life, health or security is threatened."

Other Access Exceptions

- When access may be refused (permissive):
- 9(3) "Despite the note that accompanies clause 4.9 of Schedule 1, an organization is not required to give access to personal information only if

  (*a*) the information is protected by **solicitor-client privilege**;

  (*b*) to do so would reveal **confidential commercial information**;

  (*c*) to do so could reasonably be expected to **threaten the life or security of another individual**;

  (*c*.1) the information was collected under paragraph 7(1)(*b*) (**investigation** of a breach of an agreement or contravention of the laws of Canada or of a province); or

  (*d*) the information was generated in the course of a **formal dispute resolution process**.

  However, in the circumstances described in paragraph (*b*) or (*c*), if giving access to the information would reveal confidential commercial information or could reasonably be expected to threaten the life or security of another individual, as the case may be, and that information is severable from the record containing any other information for which access is requested, the organization shall give the individual **access after severing**.

  (4) Subsection (3) does not apply if the individual needs the information because an individual's life, health or security is threatened."

Access Exceptions

- If you are requested access to information that has been disclosed to government authorities for law enforcement, national security, defence of Canada, international relations, seek immediate legal advice
- Sections 7(3)(2.1), (2.2), (2.3), (2.4) set out a requirement to not provide the information or reveal the disclosure until government has been provided an opportunity to object to the access by the individual.
- Confusingly drafted – difficult to follow.

Privacy – Obligations for Affected Organizations

- Appoint a privacy officer – needs to be well-trained
- Figure out why you collect, use and disclose personal information
  - Past practices
  - Present practices
  - Anticipate the future needs of your firm
- Determine what exemptions may apply and in what circumstances
- Create and enact policies and practices to implement the law and train staff
  - to receive and respond to complaints and inquiries from clients and the general public
  - to train staff about the firm's policies and practices
  - to enable staff to explain why specific information is being collected
- Make general policies and procedures reasonably available
- Communicate all purposes, uses and disclosures of personal information at least at the time of collection, unless an exemption is applicable
- Draft consent forms, if necessary, for collection, use and disclosure of personal information
- Draft contracts with service providers to follow the firm's policies (e.g. temp agencies, transcription services, cleaners, etc.)
- Put in place audit and disclosure mechanisms
- Protect personal information holdings with adequate security measures
- Keep up to date with changes to the law or interpretations of the law
- And more!

Action Plan

- **Appoint a privacy officer or project leader**
- **Information inventory (looking backward)**
  - What personal information do you have?
  - Do a detailed analysis of where it came from, under what circumstances, whether there was consent, etc.
  - Can you keep and re-use that personal information?
  - Was it collected on your own or your client's behalf?
- **Information plan (looking forward)**
  - Assess what information you need and why.
  - Is it all reasonable?
  - Is the information sensitive?
  - Do you get the information first-hand?
  - Consent strategy – opt-out, opt-in, or exception?
  - Limits on collection, use, disclosure and retention
- Privacy policy
  - Draft a clear, concise but specific document that communicates the firm's information management policies and practices
  - Train employees (lawyers and staff)
- Accountability / compliance challenges
  - Appoint privacy officer and make sure she is well trained
  - Put in place methods to answer or escalate questions quickly & truthfully – prevent questions from turning into complaints.
  - Put in place rigorous screening procedures so that no inappropriate information is released.