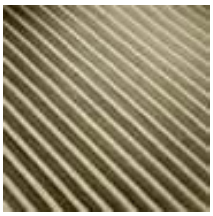
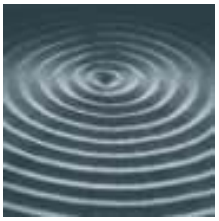


2500, 20 Queen St. West
Toronto, ON M5H 3S1
Canada
Tel. 416.595.8500
Fax.416.595.8695
www.millerthomson.com



MILLER THOMSON LLP

Barristers & Solicitors, Patent & Trade-Mark Agents

TORONTO VANCOUVER WHITEHORSE CALGARY EDMONTON WATERLOO-WELLINGTON MARKHAM MONTRÉAL

# Privacy Legislation in Ontario and its Application in the Appraisal Industry

Richard D. Leblanc

February 4, 2005

# PRIVACY LEGISLATION IN ONTARIO

# AND ITS APPLICATION IN THE APPRAISAL INDUSTRY

**by**

**Richard D. Leblanc**

**rleblanc@millerthomson.com**
**416.595.8657**

**Presented at**

**FEE APPRAISERS' SYMPOSIUM 2005**

**ONTARIO ASSOCIATION OF THE APPRAISAL INSTITUTE OF CANADA**

**Holiday Inn on King**

**370 King Street West, Toronto, Ontario**

**Friday, February 4, 2005**

MILLER THOMSON LLP

Barristers & Solicitors, Patent & Trade-Mark Agents

**Discussion Questions:**

1. **Are interior/exterior photographs of a subject property considered personal information?**

2. **What steps should be taken to protect the firm respecting credit card orders over the telephone?**

3. **Is MLS information personal information?**

4. **Can MLS data be stored for future comparison purposes? Can this information be used to produce automated valuations?**

5. **Is the data in a fee appraiser's database personal? Can it be shared within the office? Can it be disclosed outside the office?**

6. **In the Bank/appraiser relationship, who is the client, and who needs to provide consent?**

7. **Are fee appraisers required to review information in existing databases and obtain consents for use in comparisons?**

8. **Is our client list "personal information"? Can we sell it to third parties for a fee?**

9. **If someone wants to buy my practice, can I show them my client list?**

10. **Is a municipal address personal information?**

## A. Introduction to Privacy Issues

### 1. General

Traditionally, the right of an individual to privacy has meant the right "to be left alone." A fundamental tenet of existence in Western democratic society is the desire and expectation to be free from unwanted intrusion into one's life and personal affairs by others. Specifically, this translates to the desire to maintain the privacy of one's personal property, the desire not to have undesirable facts about oneself disclosed to the public, and the right not to have one's personality appropriated for the benefit of others. Laws of general application, such as the law against trespass to property, laws of libel and slander, intellectual property laws and the privacy rights afforded under certain provincial statutes are rough instruments which have been of some use in protecting the individual's broader rights to privacy[1].

The proliferation of personal computers, the growth of the internet and the explosion of e-commerce in recent years has spawned a different form of privacy interest with somewhat chilling implications. Data mining techniques combined with unprecedented computing power have enabled mass marketers and advertisers to collect and manipulate volumes of highly detailed information about individuals and their preferences for their own benefit and for the benefit of other commercial interests. These databanks of personal information are one of the star products of the "new economy" and have allowed mass marketers to develop innovative direct marketing techniques which target individual consumers and specific demographic segments with remarkable accuracy. What is "chilling" is that more often than not, this data is collected without the knowledge or consent of the consumer, and often contains information that the consumer would not have voluntarily surrendered without knowledge of its future use. Big Brother is, in fact, watching you, and Big Brother is everywhere[2].

While international legislation governing the protection of personal information has been in progress for some time[3], it was not until January 1, 2001 that Canada's privacy legislation, the *Personal Information and Protection of Electronic Documents Act* ("PIPEDA" or the "Act")[4] came into effect. At that time, Part I of the Act was activated to regulate the collection, use and disclosure of personal information by federal works, undertakings or businesses, and by certain organizations engaged in inter-provincial activities. On January 1, 2004, the remainder of the Act came into effect and has since applied to organizations which use, collect and disclose personal information in the course of their commercial activities. The Act applies in all Canadian provinces which do not have their own privacy statute. At the time of writing, Quebec, British Columbia and Alberta have adopted provincial laws which are substantially similar to the Act. Ontario does not yet have its own privacy legislation and hence PIPEDA applies.

---

[1] *Privacy Acts* of B.C., Manitoba, Newfoundland and Saskatchewan: R.S.B.C. 1996, c.373; R.S.M. 1970, C.74; R.S.N. 1990, C. P-22; R.S.S. 1979, C. P-24; Consumer Reporting Act, R.S.O. 1990, c. C.33, etc.

[2] The USA PATRIOT ACT of 2001 for example, provides the U.S. government with the right to access information in the U.S. under outsourcing arrangements without the knowledge or consent of the affected individual.

[3] The European Union adopted Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "EU Data Directive").

[4] S.C. 2000, c.5.

### 2. Privacy and Fee Appraisers

The appraisal industry collects, uses and discloses information for the purpose of establishing and supporting evaluations of commercial and residential real property. Information is routinely collected from individuals, databases (such as MLS), institutional clients such as banks and other third parties. This information is used in the process of comparative analysis by the appraiser and is disclosed or relayed back to the client or other third party. The use of personal information is often incidental to the task of providing an appraisal where the principal information might simply be the address, the attributes of a particular building and the name of the builder. Notwithstanding this fact, the property appraiser does collect, use and disclose personal information in the context of his or her work and must therefore ensure compliance with PIPEDA.

## B. Privacy Laws

### 1. General Principles

The following common principles underpin PIPEDA and privacy laws generally:

- Personal information is to some extent personal property;
- An individual has the right to be informed of any proposed collection, use or disclosure of his or her personal information;
- An individual must consent to the collection, use or disclosure of his or her personal information;
- An organization which uses, collects or discloses personal information must do so only for the purposes stated and must maintain the security of the information; and
- Organizations which use personal information are accountable for its use and must ensure that personal information is accessible to individuals and capable of being corrected, challenged or deleted if required.

### 2. PIPEDA

#### (a) CSA Principles

The foregoing principles are embodied in Schedule 1 of the PIPEDA, which is based upon the Canadian Standards Association *Model Code for the Protection of Personal Information* (the "CSA Model Code"). Schedule 1 sets out the 10 general privacy principles originally developed by the Organization for Economic Cooperation and Development ("OECD"). These are stated as follows[5]:

[5] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as adopted by the OECD on September 23, 1980.

**Principle 1 - Accountability**

The organization must designate an individual or individuals who are accountable for the organization's compliance with PIPEDA. The organization is specifically held responsible for information that has been transferred to a third party for processing, which must be protected by contractual means. Organizations are required to implement policies and practices to give effect to the principles, including training staff.

**Principle 2 - Identifying Purposes**

The purposes for which personal information is collected must be documented and must be identified to the individual at or before the time that it is collected. Once this has been done the personal information cannot be used for a new or further purpose without the consent of the individual.

**Principle 3 - Consent**

This Principle is generally regarded as the key to the protections in PIPEDA, and will be further discussed later in this paper.

Personal information cannot be collected, used or disclosed without the informed consent of the individual, unless there is a specific exemption provided for in PIPEDA. An organization may not, as a condition of the supply of a product or service, require such consent beyond what is required for a legitimate fulfilment of the transaction. The form of consent may be explicit or implicit, or "opt-in" or "opt-out", depending upon the sensitivity of the information. Finally consent can be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice.

**Principle 4 - Limiting Collection**

This Principle provides that the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information must be collected by fair and lawful means.

**Principle 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 it is necessary for the fulfilment of those purposes. Organizations must develop guidelines with maximum and minimum retention periods.

**Principle 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.

However the implementation of this principle depends upon the use of the information. A credit reporting agency, for example, would have an obligation to make frequent updates since the accuracy of the information can materially and negatively affect the individual's interests.

**Principle 7 - Safeguards**

Personal information is to be protected by security safeguards appropriate to the sensitivity of the information. As with consent, "sensitivity" is a key concept. The purpose of the safeguards is not just to protect against theft, but also to protect against unauthorized access, disclosure, copying or use. The methods of protection should include physical measures, such as locked filing cabinets and restricted access; organizational measures, such as security clearances and access on a "need-to-know" basis; and technological measures such as passwords and encryptions.

**Principle 8 - Openness**

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. This Principle effectively requires the use of privacy statements by organizations operating in Canada, on websites, or on other material, including printed material, through which they collect personal information. It also requires that the privacy policy developed pursuant to Principle 1 be made available to individuals. Specifically the information to be made available shall include:

a) the name or title, and the address, of the person who is accountable pursuant to Principle 1;

b) the means of gaining access to personal information held by the organization;

c) a description of the type of personal information held by the organization, including a general account of its use.

d) a copy of any brochures or other information that explain the organization's policies, standards or codes; and

e) what personal information is made available to related organizations such as subsidiaries.

**Principle 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.

In PIPEDA such disclosure includes an account of the use that has been made of the information, and an account of the third parties to which the information has been disclosed.

**Principle 10 - Challenging Compliance**

Any individual shall be able to address a challenge concerning compliance to the individual accountable for the organization's personal information.

### (b) "Personal Information" as defined in PIPEDA

"Personal information" is defined in the Act as information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization. For clarity, personal information does not include information about a corporation, but does include information about identifiable individuals retained by a corporation. It is also relevant to note that information which appears in telephone directories is publicly available, and is excluded in PIPEDA from the definition of personal information.

In a recent decision, the federal Privacy Commissioner [6] declared that business e-mail addresses were personal information and were therefore subject to the protections of the Act. This is due the express wording in the Act which fails to include e-mail addresses in the exclusion of "business card" information. Although the decision is not binding, the effect of the decision will be to reduce the incidence of unsolicited email directed to business email addresses. The unfortunate effect of this is that it fails to distinguish between email for business and email for non-business purposes.

### (c) Remedies

An individual seeking redress for a breach of his or her rights under PIPEDA may file a written complaint with the federal Privacy Commissioner. The Commissioner has a specified period of time to investigate the complaint and attempt to assist the parties in resolving the dispute. Within one year of the filing of the complaint, the Commissioner must produce a report outlining its findings and recommendations. The Commissioner is not required to prepare a report if it is determines that:

(a) the complainant should first exhaust grievance or review procedures otherwise reasonably available;

(b) the complainant could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than PIPEDA, or the laws of a province;

(c) sufficient time has elapsed where the production of a report would serve no useful purpose; or

---

[6] This decision, delivered in late 2004 is not yet publicly available. It involved a complaint made by Michael Geist against the Ottawa Renegades football team in relation to e-mail solicitations.

(d) the complaint is trivial, frivolous or vexation or without merit.

Once the report has been issued, the complainant may within 45 days apply to the Federal Court of Canada Trial Division for a hearing to deliberate the merits of the complaint and the remedies sought by the complainant. The Federal Court may order the following remedies:

(a) order an organization to correct its practices in order to comply with the Act;

(b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and

(c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

As a separate power, the Commissioner may audit the privacy practices of the organization if it has reasonable grounds to believe that the organization is contravening a provision of PIPEDA. The results of this review must be included in a report to the organization.

Certain writers are of the view that PIPEDA is not the only recourse available for an aggrieved party and that the permissive language of the statute leaves open the possibility of applying directly to the courts for a remedy.

### 3. Other Jurisdictions

Currently, each of British Columbia, Alberta and Quebec have legislation governing the collection, use and disclosure of personal information. The Quebec statute entitled *Loi sur la protection des renseignements personnels dans le secteur privé* came into effect on January 1, 1994 and was declared to be substantially similar to PIPEDA on November 19, 2003.

The laws in British Columbia and Alberta are each called the *Personal Information and Protection Act*[7] and resulted from significant collaboration between the two provinces. Both the BC Act and the Alberta Act constitute a more complete package than PIPEDA. For example, the BC and Alberta Acts each deal expressly with employee information, exclude business emails from the Acts' protection and contain exemptions for disclosures of personal information in the context of business transactions. Of notable distinction is the exemption of personal information that was collected on or before the Acts came into force. PIPEDA contains no such exclusion, a fact which has given rise to significant compliance concerns under PIPEDA in relation to archived and non-current data.

## C. Implications for Fee Appraisers

The principal concerns of businesses in Ontario have been straightforward:

---

[7] S.B.C. 2003, c.63 (the "BC Act") and S.A. Ch. P-6.5 (the "Alberta Act"). These statutes were declared to be "substantially similar" to Part 1 of PIPEDA by virtue of the *Organizations in the Province of Albert Exemption Order* and the *Organizations in the Province of British Columbia Exemption Order* dated October 12, 2004.

What is the Act?

Does it apply to me?

Do I have to comply and what if I do not?

How much will it cost me to comply?

How do I comply and what are my ongoing obligations?

**1. What is the Act?**

As noted above, the Act is federally enacted legislation which applies in the Province of Ontario to every commercial organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activities. The Act has regulated private businesses in Ontario since January 1, 2004.

**2. Does it apply to me?**

The Act applies to personal information used in commercial activities. "Commercial activities" are defined in the Act as 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 fundraising lists.

As stated above, "personal information" means information about an identifiable individual but does not include the name, title, or business address or telephone number of an employee of an organization. Such information without reference to identity, information which is not capable of identifying an individual, or information taken in the aggregate is not personal information subject to the protections of the Act. Fee appraisers will often collect, use or disclose the following personal information in the course of their business:

- Name, address, telephone number, email address;
- Age;
- Gender;
- Income;
- Credit rating and other financial details;
- Price of home;
- Ownership of home/assets;
- Interior and exterior photos of residence in some cases;
- Consumer preferences;

- Health;
- Status;
- Political or religious affiliations.

The provision of real estate appraisal services for a fee falls squarely within the definition of "commercial activity". A wide variety of personally identifiable information, ranging from residential information, photographs and telephone numbers, credit information and credit card numbers, is collected from or in relation to specific individuals. To the extent that appraisal activities take place within Ontario, then PIPEDA applies and provider of services must comply with the privacy principles set out in Schedule 1 of the Act and described above.

**3. Do I have to comply and what if I do not?**

Section 5 of PIPEDA states that every organization shall comply with the obligations of Schedule 1 of the Act. The contents of Schedule 1 which summarize the 10 privacy principles are set out above and constitute statutory obligations. Failure to comply may expose the organization to the right of an individual to file a complaint with the Privacy Commissioner in the manner stated above. If the complaint is not dealt with to the individual's satisfaction, then the individual may bring an action in the Federal Court of Canada seeking further redress in the form of a corrective order, and possibly damages for any humiliation suffered by the complainant.

**4. How do I comply and what are my ongoing obligations?**

**(a) Appoint a privacy officer:** A privacy officer needs to be appointed and educated about privacy issues.

**(b) Review current practices:** A review of current practices should be performed. Specifically, the organization should consider how personal information is collected, used and disclosed. Appropriate forms of consent should be developed. In addition, the firm should consider whether information is routinely given to third party service providers, such as payroll administrators or marketing agencies, and if so, whether appropriate consents and protections are in place.

**(c) State purposes and develop privacy policy:** A list of purposes must be developed. A privacy plan and policies should then be developed on the basis of the proposed uses. This plan should consider:

(i) Implementation of the procedures and recommendations set out herein to protect personal information;

(ii) establishing procedures to receive and respond to complaints and enquiries;

(iii) training staff and communicating to staff information about the organization's policies and practices;

(iv) developing information and to explain the organization's policies and procedures; and

(v) ensuring the accuracy of the personal information held by the organization and updating and retention policies.

**(d) Develop consents:** Consent is the key to privacy compliance. While PIPEDA establishes guidelines which must be complied with in substance and to a certain degree in form, it is critical from a compliance perspective that personal information not be used without the consent of the individual to whom it relates and only for the purposes intended and of which the individual has been made aware.

Consent can be expressed or implied and is a function of the degree of sensitivity of the information, the intention of the parties, and the reasonableness of use of the information in the circumstances.

The precise form of consent required for the handling of personal information is directly related to the sensitivity of the information. PIPEDA does not define the term, although section 4.3.4 of Schedule 1 of the Act states:

"The form of consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context."

Section 5(3) of PIPEDA also states that an organization may collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

- **Consents from Individual**

Fee appraisers will need to obtain the informed prior consent of an individual in order to use that person's personal information for the stated purpose of conducting a fee appraisal. At this stage, the information provided by the individual is quite often not what would be considered to be "sensitive" information. Accordingly, a lower threshold of consent is required and consent may be implied from the conduct of the individual. For example, an individual who is disclosing personal information when filling out a form or questionnaire will be deemed to be consenting to the disclosure and the use of the information for a purpose that is reasonably related to the related document, such as the performance of a fee appraisal. Providing information in this manner and the implication of consent would not however extend to the use of information by the recipient for a third or ancillary purpose, such as the provision of the information to a lawyer or moving company or real estate agent without obtaining additional consent for this additional purpose. Appraisers should enter into the practice of obtaining and storing records of consents to use personal information and credit card information, and should keep written records where such consents are given over the telephone.

Where an appraiser is collecting more sensitive information, such as credit card information, this disclosure and use should be accompanied by an express consent from the relevant individual.

- **Consents from Banks and other Third Parties**

Simply because information is provided to an appraiser by a third party does not mean that the appraiser has no obligations with respect to the manner of use and further disclosure of the information. PIPEDA protects the unauthorized collection, use and disclosure of personal information, and there is an onus on fee appraisers to seek confirmation from the requesting institution that all necessary individual consents were obtained for the use of the information for fee appraisal purposes.

- **Consents from MLS**

Information collected on MLS is generally subject to the consent as set out in section 11 of the standard OREA listing agreement. This consent reads as follows:

"The Seller consents to the collection, use and disclosure of personal information by the Broker for the purpose of listing and marketing the Property including, but not limited to: listing and advertising the Property using any medium including the Internet; disclosing property information to prospective buyers, brokers, salespersons and **others who may assist in the sale of the Property; such other use of the Seller's personal information as is consistent with listing and marketing of the Property**. The Seller consents, if this is an MLS® Listing, to placement of the listing information and sales information by the Broker into the database(s) of the appropriate MLS® systems(s) and acknowledges that the MLS® database is the property of the board(s) and can be licensed, resold, or otherwise dealt with by the board(s). The Seller further acknowledges that the board(s) may: distribute the information to any persons authorized to use such service which may include other brokers, government departments, appraisers, municipal organizations and others; **market the Property, at its option, in any medium, including electronic media; compile, retain and publish any statistics including historical MLS® data which may be used by licensed board members to conduct comparative market analyses;** and make such other use of the information as the board deems appropriate in connection with the listing, marketing and selling of real estate."

This paragraph contains the express consent of the individual to the inclusion of the information in the MLS database and to the distribution of the information to all members entitled to use the service, including historical MLS data used by members to conduct comparative analyses.

- **Consents from Employees**

Employee information is excluded from the application of PIPEDA. Accordingly, consent to use of employee information is generally not required in Ontario. As noted above, consent can often be implied from the course of conduct, application forms and documentation entered into between the employer and the employee. Typically, unless drug tests or other invasive means will be used by an employer to obtain information from an employee, express

consents are not typically required. However, it is good practice to obtain from an employee at the outset of any employment relationship an express consent stating that the employer may use personal information for the purposes of establishing, managing or terminating an employment relationship between the employee and the employer.

**(e) Train and educate:** The privacy officer should hold a staff training meeting to educate personnel about privacy issues. Specifically, the relevance and importance of limiting collection and use, maintaining privacy and confidentiality, and ensuring that all security measures are respected, should be communicated. All staff should have read and acknowledged the privacy policy.

**(f) Review security measures:** Security measures should be reviewed and improved if necessary.

- All databases should be protected by necessary firewalls and subject to security password access and possibly encryption;
- Network access should be restricted to individuals with a need to know;
- Individuals should be asked to ensure that they logout of the database at the end of every day so that unscrupulous third parties cannot access the database;
- Removal or transfer of data to portable media (zip and flash memory), or transfer of data to personal laptops, should be carefully supervised and restricted unless necessary;
- Sensitive physical files should be kept under lock and key (as in the case of credit card information);

**Ongoing Obligations**

In order to maintain compliance with PIPEDA and other privacy standards, internal practice standards should be developed to ensure that evidence and documentation exists for:

(i) each individual's consent, for each database and purpose;

(ii) reviews of the databases for accuracy in accordance with the sensitivity of the information;

In addition, the following practices and procedures should be adopted:

(iii) Responsibility for compliance may be better separated from responsibility for collection, use and disclosure.

(iv) Provisions should be made for the regular training of new staff, and for review and update of the policies.

(v) A response plan in the event of privacy complaint should be developed.

### 5. How much will it cost me to comply?

It is not the purpose of the statute to impose an impossible compliance cost on members of the Institute. Nonetheless, at a very minimum, an individual must be designated to understand and administer privacy, a policy and procedure must be adopted, specific uses must be written down, the policies must be made accessible to the public, security must be reviewed and updated if necessary, and retention policies must be reviewed and administered. Many resources, such as compliance materials, forms of consent and draft privacy policies are available to the public. Self-education and use of publicly available materials is the least expensive way to ensure compliance.

A more costly path is to engage professional help to assist in setting up a privacy regime in an office. This highly recommended where a high volume of sensitive personal information collected, used or disclosed and where the size of the organization mandates a more formal and structured approach to the implementation of PIPEDA and the privacy guidelines.

## D. Frequently Asked Questions

### 1. Are photographs of the subject property considered personal information?

**YES** - Any information, including the content of photographs that can be identified with a specific individual is personal information. Therefore, photos of a house's exterior and interior which are associated with an identifiable individual are protected personal information which can only be used in accordance with the reasonable uses for such photos disclosed in an organization's privacy policy or which uses are necessary and incidental to the use for which the information was volunteered by the individual. It should be noted that interior and exterior photos which are not specifically associated with an individual may not be "personal information" where they cannot be associated with a specific municipal address and which can therefore not be linked to an individual.

Note that PIPEDA seeks to ensure that the collection, use and disclosure of personal information is done for purposes that are reasonable in the circumstances. For example, it is reasonable for a person applying for mortgage financing (or attempting to sell their house on conditional upon financing terms) that a house appraisal will be required. It is also reasonable for such an assessment to be conducted not by a financing institution but by a third party service provider. The consents obtained by the Bank from the applicant, and the consents obtained by the listing agent from the vendor of the property should ultimately include consent to permit such appraisal to occur, including reasonable and necessary activities ancillary thereto, such as the taking of photographs. See the discussion above relating to the form of the consent to use embedded in the MLS documentation.

### 2. What steps should be taken to protect the firm respecting credit card orders over the telephone?

Credit card information is sensitive information. Accordingly, this information should be used only for the express purpose of obtaining payment for services rendered or to be rendered, as set out in the privacy policy. This information should be stored in a locked cabinet and should be

destroyed as soon as it is no longer required. Personnel should be instructed to take very accurate notes of all conversations authorizing this use and should ideally obtain faxed instructions of same, or instructions by email which do not contain the credit card numbers (for security reasons.)

**3. Is MLS information personal information?**

**YES -** Information collected by a real estate board under MLS for purchase or sale purposes is personal information if it relates to an identifiable individual. However, this information is typically given to MLS with consent for sale and marketing purposes under the standard listing agreement. Accordingly, the review of such information by prospective purchasers and by fee appraisers for comparison purposes is not contrary to PIPEDA. One must not lose sight of the fact that a sale of a house via MLS is ultimately a public process whereby a vendor is seeking to maximize exposure to his or her property by advertising publicly with signs, in the newspaper and on the internet. Accordingly, a limited form of consent may be implied from these acts which are inherently public in nature, and from the fact that a person's identity can often be discerned from their municipal address.

**4. Can MLS data be stored for future comparison purposes? Can this information be used to produce automated valuations?**

**YES -** As indicated above, the consent in the standard listing agreement permits the use of historical data for the purposes of comparative analysis. Accordingly, this data can be accumulated in a database and used for the reasonable purposes of comparative analysis of property values. As set out above, this information is "quasi-public" information at the time of its disclosure. If this express consent has not been obtained, then to the extent that such information is used in a limited manner, with efforts made to "anonymize" the data and remove references to individual identity, there is nothing which prevents the use of the information for the limited purposes of real estate comparison.

**5. Is the data in a fee appraiser's database personal? Can it be shared within the office? Can it be disclosed outside the office?**

**MAYBE** - If the information is limited to house size, model and builder and is not capable of identifying a specific individual, then it is not personal information and can be used or disclosed outside the office without consent. Note that if the information was originally collected with the consent of the individual who had notice of a privacy policy which expressly includes consent to use the information in a database, then this issue becomes moot. Nonetheless, it is good office practice to "anonymize" all data where personal identity is not a relevant factor in property evaluations and where an express consent to use has not been obtained.

**6. In the Bank/appraiser relationship, who is the client, and who needs to provide consent?**

The Bank is the client. However, the Bank may disclose to you personal information about an identifiable individual in the course of requesting an appraisal. It is your responsibility to obtain confirmation that the Bank had the individual's prior consent to disclose this information to you.

It is also your responsibility to use the information only for the purposes and in the manner set out in your privacy policy.

**7. Are fee appraisers required to review information in existing databases and obtain consents for use in comparisons?**

Instead of seeking the individual consent of former clients to the use of their information, you may instead wish to first assess the sensitivity of the information and whether any consent to use can be implied from practice or conduct. If the information is very sensitive (e.g. financial information relating to revenue, credit rating or financial condition) and no express consents were obtained, then you may wish to modify your database entries so that all personally identifiable features are removed from the information. Note however that this exercise should take into account the following factors: the fact that names and addresses are quasi-public information which are not typically considered to be of a highly sensitive nature; the fact that this information may lose its personal character very quickly over time, especially after a property has changed hands a couple of times; the fact that names, addresses and telephone numbers which appear in a telephone directory are public information; and (v) the fact that a person whose property is sold over MLS is generally aware that the property listing including the sale price will be maintained in MLS databases and that this information will continue to be available in the future. As a follow up measure, it would be advisable to review the MLS subscription agreement to determine what confidentiality or privacy covenants govern the use of this information.

**8. Is our client list "personal information"? Can we sell it to third parties for a fee? If someone wants to buy my practice, can I show them my client list?**

**YES** - A client list is personal information and must be held in accordance with the safeguards set out in PIPEDA. You cannot sell your client list to a third party unless you have obtained the express or implied consent of the individuals in respect of whose personal information is contained on the list. The sale of a client list is a secondary purpose and the use must have been disclosed. If someone wishes to see your client list, then you should obtain a confidentiality and privacy covenant from the prospective purchaser promising that they will not use the information for any purpose other than reasonable due diligence in connection with a proposed transaction, that they will destroy or return all information if the transaction does not proceed and that they will indemnify you for any damages or costs arising from their use of the personal information while **it is in their control or possession.**

**9. Is a municipal address "personal information?"**

**YES**, if it is in relation to an identifiable individual. However, an organization may collect, use and disclose this information if it is publicly available or consists of the name, address or telephone number of a subscriber that appears in a telephone directory that is available to the public. This use must however be reasonable in the circumstances.

**10. Other questions.**

## Schedule A

### GENERIC PRIVACY POLICY FOR USE BY MEMBERS OF THE APPRAISAL INSTITUTE OF CANADA

### 1. Privacy Statement

As a member of the _____ Association of the Appraisal Institute of Canada (the "**AIC**"), _____ [**I am/we are**] committed to respecting the confidentiality and privacy of personal information provided to us by our employees and by our clients. [**I/we**] have adopted the ten privacy principles set out in the Canadian Standards Association *Model Code for the Protection of Personal Information* and embodied in the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"). [**I/we**] observe our obligations under PIPEDA, under provincial legislation in effect in Quebec, British Columbia and Alberta to the extent applicable, and under such other applicable provincial privacy laws which are substantially similar to PIPEDA as may come into force from time to time. [**I/we**] will collect, use and disclose personal information only for such purposes and to such extent as is necessary to enable us to provide our services as professional real estate appraisers and to fulfill our roles as active members of the AIC.

### 2. Definition of Personal Information

Personal information is information about an identifiable individual but does not include the name, title or business address or telephone number of an employee of a business. Personal information includes personally identifiable information such as a person's home address and residential contact information, age, gender, income, credit rating, financial information, consumer preferences, health status and political affiliations. For the purposes set out in this privacy policy, appraisal information which has been obtained from or in relation to an individual should be treated as "personal information" where such information is of a type which may reasonably be used to identify a specific individual, and including information which contains the name and/or residential address of the individual, or contains, for example, an identifiable photograph of a person's residence. This is due to the fact that an individual's identity can often easily be identified in correlation with such identifiable information.

### 3. Purposes of Use of Personal Information

[**I/we**] collect personal information for the sole purpose of enabling **[us/me]** to perform independent real estate appraisals for our clients. In the course of performing these services, [**I/we**] will require the name, address (including both business and home addresses on occasion), business, cell, fax and home telephone numbers and email addresses of identifiable individuals. [**I/we**] may also require in certain circumstances information relating to the purchase price paid for real property, the details of any real estate transaction relating to a subject property, details of any lease transaction and documentation relating to a subject property, financial information relating to repairs or renovations on a subject property, individual credit history, income and other sensitive financial personal information of identifiable individuals. Once an appraisal report has been delivered to a client, the information in the report will be added to a database of information containing other archived reports. The member will either render these records anonymous by removing from any appraisal report all information which is reasonably capable

of identifying an individual, or will obtain the express consent to the future use by the member of such client's personal information.

## 4. Manner of Collection, Use and Disclosure of Personal Information

As noted above, [**I/we**] will only collect, use and disclose personal information for the purposes of providing services to our clients, and for purposes ancillary thereto, such as billing and collection of accounts in respect of which credit has been extended. [**I/we**] will collect personal information in personal interviews, from letters of instruction, from order forms, from financial institutions and from other business contacts or real estate agents. By providing us with such information, individuals are deemed to consent to its use for the purposes set out herein. When [**I/we**] receive personal information from other businesses, [**I/we**] will treat such personal information in a manner consistent with this policy. When [**I/we**] require sensitive financial personal information, or other information of a particularly sensitive nature, [**I/we**] will seek to confirm that consent was given for the disclosure of such information prior to collecting, using or disclosing such information.

[**I/we**] will not use personal information for any other or secondary purpose. Specifically, [**I/we**] will not provide personal information, either by way of sale or other disclosure, to any marketing agency, mailhouse, data processing agency or any other promotional entity without express written consent. [**I/we**] will not collect information which [**I/we**] do not require in the course of providing our services. [**I/we**] may retain personal information for the purposes of building and supplementing my appraisal database. [**I/we**] will not provide to present clients personal information relating to former clients without obtaining the express consent of any such former client.

## 5. Retention and Disposal of Personal Information

[**I/we**] will not retain personal information longer than is necessary for the purposes of serving our clients hereunder and as otherwise required by legislation. Specifically, certain appraisals are made for mortgage lending purposes and for tax valuation purposes and accordingly, [**I/we**] retain such information and personal information forming the basis of such information for periods equal to the reassessment limitations periods imposed by tax legislation, to comply with our insurance requirements, and as otherwise required to comply with applicable laws. In general, [**I/we**] will retain client files and personal information therein for a period of [●____] years, after which time we will no longer need to retain such information. When [**I/we**] no longer have any use for the personal information, [**I/we**] dispose of it by having it shredded or destroyed in the case of physical files and documents, and by erasing the files from our hard drive or other storage medium in the case of electronic data files.

## 6. Protection and Security of Personal Information

[**I/we**] have implemented policies and procedures to ensure that personal information is protected from unauthorized access, use, tampering, loss or disclosure. Firstly, only those who will be involved in the provision of the services will have access to personal information. Secondly, all personal information which is retained on our computers will be stored in secure folders and will

not be available for general access in our organization. All computer and information systems with internet access will be equipped with firewalls, antiviral software and power source back up to ensure the security and integrity of your personal information.

In the event that [**I/we**] require the services of third parties and need to provide personal information to such third party for the purposes of providing our services, [**I/we**] will first confirm that consent has been provided to so disclose the information. Upon confirming the relevant individual's consent, [**I/we**] will not provide such information until [**I/we**] receive reasonable assurances from any such third party that they have in place a privacy policy which is substantially similar to this policy.

## 7. Review of Accuracy of Personal Information on File

If an individual has a concern with the accuracy or contents of their personal information which we have on file, such individual may contact our privacy officer to request particulars of his or her personal information. Any such request must be made in writing and addressed to the privacy officer at the address set out below. The privacy officer shall review such request and endeavour to respond within 30 days. The privacy officer may refuse to provide this information to the individual if so providing it would result in disclosure of personal information about a third party who has not consented to such disclosure. The privacy officer may also refuse to provide such information where such information: is protected by solicitor-client privilege; cannot be separated from confidential commercial information; the disclosure of which would result in the breach of an agreement or of a law of Canada or one of its provinces. The privacy officer may request that the individual provide documentation or evidence to support the challenge to the accuracy of the personal information on file. The privacy officer reserves the right to review such documents and evidence and shall upon being convinced of error or inaccuracy, amend the individual's personal information accordingly.

## 8. Privacy Officer

In order to review personal information, to express any concern relating to privacy or review our compliance with this privacy policy or any relevant federal or provincial privacy legislation, an individual may contact [**me/us**] by mail, email or telephone at the contact information set out below:

[Name of Practitioner/Individual Appointed as Privacy Officer]
**Attention: Privacy Officer**
[Organization]
[Address]
[Email information]
[Telephone contact information]

More general information may be found on the website of the Information and Privacy Commissioner of Canada at www.privcom.gc.ca. The Commissioner can be reached by mail at 112 Kent Street, Ottawa, Ontario, K1A 1H3, and toll free by phone at 1-800-282-1376.

**Schedule B**

**GENERIC CONSENT FORM**
**FOR USE BY INDIVIDUAL CLIENTS OF MEMBERS OF**
**THE APPRAISAL INSTITUTE OF CANADA**

**To: [Name of Member Organization]**

**[*Note: The contents of this letter may be added to a standard engagement letter/order form, or may be customized to add general retainer or engagement language such that only one and not two forms are necessary for each engagement.*]**

I acknowledge that I have engaged you to provide appraisal services to me [***on the terms set forth in the aforementioned retainer***.] I acknowledge that in the course of this engagement I will provide you with certain confidential personal information. I acknowledge having been given the opportunity to review your Privacy Policy. I consent to the collection, use and disclosure by you of my personal information but only in the manner, for such purposes and for such time as are set out in your Privacy Policy and for no other reason or uses except as may be required by law. **[*Specifically, I consent to the inclusion of my personal information in your database for future use in performing comparative valuations of properties similar to mine.*]**

I understand that I may contact your Privacy Officer at any time at [***privacy@member.com***] should I have any concerns relating to the collection, use or disclosure of the personal information disclosed to you in connection with this engagement.

Dated this ____ day of _____, 200___.

By:_____
Name:

**[Note: Privacy Policy may be attached as a schedule. This may be appropriate for retainers with financial institutions.]**

**Schedule B-1**

**GENERIC STANDING CONSENT FORM**
**FOR USE BY INSTITUTIONAL CLIENTS OF MEMBERS OF**
**THE APPRAISAL INSTITUTE OF CANADA**

**To: [Name of Member Organization]**

**[*Note: The contents of this letter may be added to a standard engagement letter/order form, or may be customized to add general retainer or engagement language such that only one and not two forms are necessary for each engagement. Note that financial institutions may have their own form of contract or consent which they will use to bind members to the terms of their own privacy policy.*]**

We acknowledge that we have engaged you to provide appraisal services to us from time to time. We acknowledge that in the course of these engagements we may provide you with certain confidential personal information relating to our clients. We acknowledge having been given the opportunity to review your Privacy Policy. We consent to the collection, use and disclosure by you of such personal information but only in the manner, for such purposes and for such time as are set out in your Privacy Policy and for no other reason or uses except as may be required by law. Specifically, we consent to the inclusion of such personal information in your database for future use in performing comparative valuations of properties provided that any information identifying a particular individual is deleted from your records. Such information includes specifically the name of any particular individual and the street address number relating to an individual.

We understand that we may contact your Privacy Officer at any time at [***privacy@member.com***] should we have any concerns relating to the collection, use or disclosure of the personal information disclosed to you in connection with this engagement.

Dated this ____ day of _____, 200___.

By:_____
Name:

## Schedule C

### STATEMENT FOR PRINTED MATERIALS AND REPORTS

**1. Statement to be added to forms or printed materials in which personal information is collected from individual clients.**

**[Insert Name]** takes privacy very seriously. We collect personal information to better serve our customers, for security reasons, and to provide customers and potential customers with information about our services. We would like to have a lifelong relationship of good service with our customers, and for that reason we may retain any personal information provided for as long as necessary to provide our services and respect our obligations to governmental agencies and other third parties. By completing this form you are consenting to our collecting and retaining this information. The information will remain confidential to **[Insert Name]**, to businesses working for us, and to any organization that acquires part or all of our business, provided that they agree to comply with our privacy policy and notify you of material changes.
If you wish access to your personal information, wish to see our Privacy Policy, or have privacy questions or concerns, please contact the **[insert name]** Privacy Officer at by phoning **[Insert phone number]** or by e-mail at: **[Insert email address]**. You may also request that your personal information be corrected or your consent to our maintaining or disclosing your information be withdrawn, except where otherwise required by law.

**2. Statement to be added to reports provided to financial institutions and third parties.**

**[Insert Member Name]** takes privacy very seriously. We collect personal information to better serve our customers, for security reasons, and to provide customers and potential customers with information about our services. We would like to have a lifelong relationship of good service with our customers, and for that reason we may retain any personal information provided for as long as necessary to provide our services and respect our obligations to governmental agencies and other third parties. The information will remain confidential to **[Insert Member Name]**, to businesses working for us, and to any organization that acquires part or all of our business, provided that they agree to comply with our privacy policy. By accepting this report, you are agreeing to maintain the confidentiality and privacy of any personal information contained herein and to comply in all material respects with the contents of our Privacy Policy. If you wish to see a copy of our Privacy Policy, or have privacy questions or concerns, please contact the **[Insert Member Name]** Privacy Officer at by phoning **[Insert phone number]** or by e-mail at: **[Insert email address]**.

**3. Employee consent form to be obtained from employees.**

**Employee Privacy Statement**

As your employer, **[Insert Member Name]** must collect and use personal information about you as its employee to ensure the efficient, safe, secure and competitive operation of its business, to provide remuneration and benefits, and to comply with regulatory requirements. This includes monitoring the volume and content of e-mails and use of the internet to ensure the efficient operation of its computer network in compliance with the law and its workplace policies. **[Insert Member Name]** will make a reasonable effort to avoid monitoring the content of personal e-mails marked as such. However **[Insert Member Name]** reserves the right to monitor e-mails sent to other employees under all circumstances.

**[Insert Member Name]** discloses employee personal information, on a need-to-know basis, to government agencies as required, to third party suppliers of services to **[Insert Member Name]**, provided that such suppliers agree to adhere to **[Insert Member Name]**'s Privacy Policy, and to prospective purchasers of all or part of **[Insert Member Name]** business.

**[Insert Member Name]** reserves the right to collect, use and disclose further personal information for these or other reasonable purposes, provided that it notifies you in advance of such activity and its purpose.

To access your personal information held by **[Insert Member Name]**, to obtain a copy of **[Insert Member Name]**'s Privacy Policy, or if you have other questions or concerns, please contact **[Insert name of privacy officer]**.

**Signed** this ___ day of _____, 200___.

| | |
|---|---|
| Witness | **NAME** |