



Office of the  
Privacy Commissioner  
of Canada

A PRIVACY HANDBOOK FOR LAWYERS

# PIPEDA and Your Practice







# TABLE OF CONTENTS

<b>INTRODUCTION .....</b>	<b>1</b>
Lawyers and privacy .....	1
Scope of this handbook .....	1
Application of PIPEDA .....	1
Requirements of PIPEDA .....	2
What constitutes “personal information” under PIPEDA? .....	2
What constitutes “commercial activity” under PIPEDA? .....	2
Knowledge and consent under PIPEDA .....	3
Office of the Privacy Commissioner of Canada .....	3
<b>PRIVACY ISSUES IN MANAGING A LAW PRACTICE .....</b>	<b>4</b>
Overview .....	4
Collection of personal information .....	4
Use and disclosure of personal information .....	5
Providing access to personal information .....	6
Safeguarding personal information .....	7
Retention of personal information .....	8
Data breaches .....	8
Employee personal information .....	9
International issues .....	10

<b>PRIVACY ISSUES IN CIVIL LITIGATION</b> .....	<b>11</b>
Application of PIPEDA to litigation .....	11
Express consent, implied consent and exceptions to consent .....	12
Privacy issues arising in preparation for litigation .....	13
Privacy issues arising in the course of litigation .....	15
Access requests and litigation .....	18
<b>CONCLUSION</b> .....	<b>19</b>
<b>ENDNOTES</b> .....	<b>20</b>

# INTRODUCTION

## Lawyers and privacy

Lawyers regularly handle sensitive personal information in running their practice and in the course of representing clients. They are accustomed to maintaining the confidentiality of information imparted to them in their professional capacity. Rules of professional conduct, rules of court and other rules and regulations have long imposed such obligations on lawyers. Law societies and professional insurers provide additional guidance, including in relation to practice management, the law of privilege, file retention, access to and ownership of files, among other issues.

Like other organizations in Canada, law practices must also comply with applicable privacy legislation. The requirements of privacy laws, including the *Personal Information Protection and Electronic Documents Act* (PIPEDA) where applicable, must be considered by lawyers in connection with any collection, use or disclosure of personal information, or access to such information.

Given their unique role when acting on behalf of clients, lawyers must also be aware of the privacy laws that may apply to the clients they represent, particularly in civil litigation. Privacy laws applicable to clients can shape and restrict the activities that lawyers may engage in on their behalf.

## Scope of this handbook

This handbook is intended to provide an accessible overview of the requirements of PIPEDA as it may apply to lawyers and law firms in private practice and some corporate counsel. It is designed to help lawyers maintain best practices in managing their collection, use and disclosure of personal information, and access thereto, in compliance with PIPEDA standards. This handbook also addresses the potential application of PIPEDA in the civil litigation context.

The focus of this handbook is on PIPEDA. It does not address the privacy requirements that may apply to crown counsel and public sector lawyers. Nor does this handbook address other provincial private sector privacy laws that may apply to some lawyers or their clients.

As well, criminal proceedings and proceedings before administrative tribunals are not covered here.

## Application of PIPEDA

PIPEDA applies to organizations that collect, use or disclose personal information in the course of commercial activities, including federal works, undertakings and businesses. Given the nature of their activities, this would include private sector lawyers and law firms, and in many cases, their clients.

PIPEDA also applies to federal works, undertakings and businesses in respect of employee personal information. Organizations located in Yukon, Nunavut and the Northwest Territories are considered to be federal works, undertakings and businesses.

In general, PIPEDA applies to organizations' commercial activities in all provinces, except organizations that collect, use or disclose personal information entirely within Alberta, British Columbia or Quebec (or Ontario, in respect of personal health information collected, used or disclosed by health information custodians; PIPEDA otherwise covers commercial activities in Ontario). In such cases, it is the substantially similar provincial law that will apply instead of PIPEDA, although PIPEDA continues to apply to interprovincial or international transfers of personal information.

## Requirements of PIPEDA

Generally speaking, PIPEDA seeks to balance the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information in the course of carrying out their business. PIPEDA requires organizations to comply with a set of legal obligations based on the following ten principles:

- Accountability
- Identifying purposes
- Consent
- Limiting collection
- Limiting use, disclosure and retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance

Furthermore, subsection 5(3) of PIPEDA provides that organizations may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. Lawyers should consult PIPEDA for more details regarding the applicable obligations and requirements.

## What constitutes “personal information” under PIPEDA?

PIPEDA applies to the collection, use and disclosure of “personal information.” This term is broadly defined as “information about an identifiable individual,” excluding “the name, title or business address or telephone number of an employee of an organization.”

It is not always straightforward to determine whether or not information is “personal information” for the purposes of PIPEDA. As per relevant jurisprudence on the concept of “personal information,” a broad and expansive interpretation is in order. Information will be “about” an individual when it is not just the subject of that individual, but also relates to or concerns the individual.<sup>1</sup> An individual will be “identifiable” where there is a serious possibility that they could be identified through the use of that information, alone or in combination with other available information.<sup>2</sup>

## What constitutes “commercial activity” under PIPEDA?

Subsection 2(1) of PIPEDA defines “commercial activity” as any “transaction, act or conduct or any regular course of conduct that is of a commercial character.” In one case, the Federal Court of Appeal confirmed that a professional activity may constitute a commercial activity. In that case, the Court held that when a doctor conducts an independent medical examination of an insured

person on behalf of, and is paid by, an insurance company, for the purpose of processing a claim for insurance benefits, he does so “in the course of a commercial activity.”<sup>3</sup> The Assistant Commissioner has also found that law firms were engaged in a commercial activity where a law firm sought a credit check on potential clients, and has determined that clients have a right of access to their personal information under the control of their lawyer.<sup>4</sup>

## Knowledge and consent under PIPEDA

PIPEDA requires individuals’ knowledge and consent in respect of every collection, use and disclosure of personal information covered by PIPEDA, unless an exception applies.

An organization must identify and document the purposes for which it seeks to collect personal information at or before the time of collection. Organizations will typically seek consent for the collection and subsequent use or disclosure of the personal information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before it is used or disclosed (for example, when an organization wants to use information for a purpose not previously identified).

Consent under PIPEDA must be meaningful, which means that organizations must make a reasonable effort to ensure that individuals are advised of the purposes for which the information will be collected, used or disclosed. Purposes must be explained in such a manner that the individual can reasonably understand how the information will be used or disclosed.

Consent under PIPEDA can also be express or implied. The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information.

Organizations must take into account the sensitivity of the information in determining the form of consent to be sought. The reasonable expectations of the individual are also a key consideration.

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice; the organization must inform the individual of the implications of such withdrawal.

## Office of the Privacy Commissioner of Canada

At the Office of the Privacy Commissioner, we understand that lawyers face unique privacy challenges on a daily basis as they manage their own personal information practices, as well as advise clients on how best to manage theirs. Part of our mandate is to help guide stakeholders, including lawyers, on how to respect their PIPEDA obligations in the course of carrying on their business. Individuals have the right to complain to the Office of the Privacy Commissioner about the personal information management practices of organizations, and the Commissioner herself may initiate a complaint based on reasonable grounds.

Upon completing her investigation of a complaint under PIPEDA, the Commissioner can make findings and issue non-binding recommendations where appropriate. Individuals or the Commissioner may then proceed to Federal Court to seek legal enforcement, if necessary.

For more information about the Commissioner’s role, and for access to the Commissioner’s findings under PIPEDA and other useful information, lawyers are encouraged to visit the Commissioner’s website at [www.priv.gc.ca](http://www.priv.gc.ca).

# PRIVACY ISSUES IN MANAGING A LAW PRACTICE

## Overview

Lawyers must ensure that they comply with all of the general requirements of PIPEDA. The starting point for compliance with PIPEDA for many law firms is the appointment of an individual who will be accountable for the organization's compliance with the Act, such as a chief privacy officer. Smaller firms and sole practitioners also need to identify an individual to assume responsibility under PIPEDA for privacy compliance. In the case of sole practitioners, they will be required to assume this responsibility themselves.

Lawyers and law firms must understand how personal information is collected, used and disclosed in the course of running the practice, and for what purposes. Privacy policies and practices must be developed and implemented to address the various ways that personal information is handled, including obtaining consents as needed and developing procedures to handle complaints and requests for access to personal information under PIPEDA.<sup>5</sup>

Although there is no "one-size-fits-all" approach to privacy compliance for lawyers and law firms, the following sections highlight some of the issues that commonly arise in practice.

## Collection of personal information

Lawyers may need to collect certain personal information from potential or existing clients in order to perform the required conflict checks prior to opening a new file. Law Society requirements may also require the collection of certain identification information from the individual client(s) for the purposes of securing a retainer. Knowledge and consent of individuals will be required in such cases. The purposes for which personal information will be collected and subsequently used should be explained to the individual(s). Typically, individuals who contact a lawyer in search of legal services will give either express consent to such collection, or implied consent through the act of providing the requested information to the lawyer in order for the conflict check to be conducted or the retainer to be secured.

Lawyers may also collect personal information about a client or prospective client from sources other than the individual. For example, some lawyers conduct a credit check on a prospective client before agreeing to represent the client. Such checks require the express consent of the individual. In terms of managing financial risk, however, lawyers should consider less privacy-invasive alternatives available to them, including the common practice of asking for a retainer amount from the client.

As well, lawyers should only retain the personal information of potential clients for as long as is needed to finalize a retainer, including resolving any potential conflicts of interest. While a lawyer may want to document having consulted with an individual and the reasons for not taking on a certain case, lawyers should consider minimizing the amount of personal information they retain following such consultations to address potential conflict issues. Different retention considerations may apply once a lawyer is retained.

## Use and disclosure of personal information

Like many organizations, lawyers will often market their services using information about clients, prospective clients and others. Often this involves only business contact information. However, it may sometimes involve the use of individuals' personal information (e.g. birthdays, personal interests, relationships between existing clients and new referrals, etc.). In cases where personal information is used or disclosed by lawyers for a secondary purpose, that is, for a purpose other than that for which the personal information was initially collected, lawyers must obtain the consent of the affected individuals. For example, where personal information was originally collected for the purpose of giving legal advice, a lawyer must obtain further consent to the subsequent use of the information for a secondary purpose, such as marketing. Where a lawyer seeks to use personal information for a secondary purpose, the lawyer should determine the appropriate form such consent should take. An "opt-in" form of consent requires an individual to express positive agreement, while an "opt-out" form presumes consent until the individual withdraws it.

Lawyers should advise individuals of the potential for their personal information to be used or disclosed for

any secondary purpose. One example of a secondary use of personal information where opt-out consent may be appropriate under PIPEDA is for marketing purposes. However, for opt-out consent to be valid in such circumstances, the Office of the Privacy Commissioner has offered the following guidance:

- The personal information must be clearly non-sensitive both in terms of its nature and the context in which it is purported to be used.
- The organization intending to use or disclose personal information for marketing purposes must limit and clearly define the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.
- The organization's purposes for using or disclosing personal information for marketing purposes must be limited and well-defined, stated in a reasonably clear and understandable manner, and brought to the individual's attention at the time the personal information is collected, or prior to the subsequent use or disclosure.
- The organization using or disclosing personal information for marketing purposes must establish a convenient procedure for easily, inexpensively, and immediately opting out of, or withdrawing consent to, secondary purposes and must notify the individual of this procedure either at the time the personal information is collected, or prior to the secondary use or disclosure of the information.<sup>6</sup>

Lawyers sometimes receive personal information from clients or others about individuals that may be in need of legal services. Lawyers should not necessarily assume that their clients, or others, have obtained the consent of a prospective client to be contacted by a lawyer. Lawyers should instead encourage clients referring another individual that may be in need of legal advice to invite that individual to contact the lawyer. Any collection,

use or disclosure of the information should not be undertaken by the lawyer until contact has been made and the lawyer may assess the scope of any express or implied consent from the individual.

Lawyers must guard against any inadvertent disclosure of personal information about their clients, including in conversations with others and in papers or conference presentations. In addition to strong professional rules of confidentiality that prevent such disclosures, PIPEDA also prohibits such disclosures of personal information without consent. In most cases the affected individuals cannot be considered to have given implied consent to such disclosures and only express consent will be acceptable.

Ultimately, lawyers should be conscious of limiting the disclosure of any personal information they may have. As a best practice, lawyers preparing newsletters or giving presentations at conferences should give thought to anonymizing or de-identifying personal information in any case law or resources they rely on. Most times, the identity of an individual need not be disclosed in order to explain the legal reasoning underlying a decision.

Lawyers occasionally find themselves sought after by law enforcement authorities, regulatory agencies and others in search of information about their clients. Strict professional responsibilities of confidentiality may prevent or restrict a lawyer from disclosing any client information in such circumstances. For its part, however, PIPEDA permits (though does not require) organizations to disclose personal information about individuals without their knowledge or consent upon the request of a government institution with the requisite lawful authority to enforce or administer a law of Canada or of a province. PIPEDA also permits organizations to disclose personal information about individuals as required by law.

## Providing access to personal information

PIPEDA provides that, upon written 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. Individuals may also challenge the accuracy and completeness of the information and have it amended as appropriate.

PIPEDA requires organizations to respond to access requests within 30 days (or other deadline set in accordance with section 8 of PIPEDA). As PIPEDA requires organizations to provide access at minimal or no cost, lawyers should not charge any fees for the time it took them or their administrative staff to respond to access requests.

Lawyers and law firms must develop policies and procedures to address access and accuracy. For example, when correcting inaccurate information, lawyers must transmit the amended information to any third parties having access to the information in question, where and as appropriate.

In responding to an access request, lawyers must provide the requested information in its integrity and not just in summary form. In responding to an access request under PIPEDA, an account must also be provided of the use that has been made or is being made, and of any disclosures that were or may have been made to third parties.

Lawyers may refuse to provide access to personal information in a number of limited situations, as listed under subsection 9(3) of PIPEDA. These include situations where: the information is protected by solicitor-client privilege; to do so would reveal confidential commercial information; the information was collected without consent in the course of an investigation into the breach of an agreement or of a law of Canada or of a province;

and the information was generated in the course of a formal dispute resolution process.

Subsection 9(3) of PIPEDA provides an exhaustive list of the circumstances in which access to personal information may be refused. In one case, for example, the Commissioner concluded that solicitors must comply with their obligations to grant individuals access to their personal information, notwithstanding the existence of a valid solicitor's lien.<sup>7</sup>

Lawyers should also be aware of subsections 9(2.1) to 9(2.4) of the Act, which may limit the information to which an individual may have access in certain limited circumstances involving disclosures to some government institutions.

Severances must be considered in certain circumstances. Any refusals of access must be made in writing, setting out the reasons and the recourses available. As well, lawyers can also choose to make sensitive medical information available through a medical practitioner.

Lawyers must not give an individual access to personal information if doing so would likely reveal personal information about a third party, unless: the third party's personal information can be severed from the rest of the information; the third party consents to the access; or the information is needed because an individual's life, health or security is threatened.

## Safeguarding personal information

Lawyers are familiar with the need to safeguard their clients' information. However, like all organizations, work options available to lawyers have evolved considerably. In the course of their practices, lawyers and support staff often work using computers, laptops, smart phones and other mobile devices. The use of such devices presents a number of challenges in safeguarding personal information.

Lawyers can face a number of potential vulnerabilities in the course of their practice, including the following:

- poor security measures for paper documents, computer systems, computer applications, mobile devices, computer networks, wireless networks or email transmission;
- misplacing paper or electronic documents;
- traces left by electronic documents (i.e. metadata)
- insecure courier/postal communication; and
- third-party suppliers and partners may mishandle information (including third-parties offering cloud computing services).

PIPEDA requires personal information to be safeguarded at all times. Personal information should be safeguarded through the use of:

- physical measures, for example, locked filing cabinets and restricted access to offices;
- organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
- technological measures, for example, the use of passwords and encryption.

The more sensitive the information is, the stronger the safeguards must be.

One measure to ensure that personal information is secured is to avoid physically removing the information from the office at all, or to limit doing so to the greatest extent possible. There are many technological solutions that allow lawyers to securely access office systems remotely. Such solutions, provided they are implemented in a secure manner and employ appropriate encryption standards and firewalls, can offer the best protection for personal information.

Any laptops and other mobile devices and media must be secured, including through the use of encryption. Highest care must also be taken when working in public spaces or on devices to which more than one person may have access. As well, lawyers or law firms considering cloud computing solutions must carefully consider the privacy and security implications of any service they may create or subscribe to.

Lawyers must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Where any third party service provider may have access to or otherwise handle personal information on behalf of a lawyer, including cloud computing service providers, it is strongly recommended that a written agreement be put in place between the third party and the lawyer. Such a contract should include provisions governing the jurisdiction where information will be processed or stored, ownership and use of information, the level of privacy controls used by the service provider, access and correction procedures, audits, and deletion procedures. Lawyers must remember that they remain accountable for information transferred to third parties for processing. PIPEDA also requires organizations to be transparent about their personal information handling practices. Accordingly, organizations should notify clients when using a service provider located outside Canada and advise them that their personal information may be subject to the laws of a foreign jurisdiction.<sup>8</sup>

The Office of the Privacy Commissioner has developed a self-assessment tool to assist organizations measure how well they are safeguarding personal information.<sup>9</sup>

## Retention of personal information

As handlers of personal information, lawyers have an obligation to ensure that they retain personal

information only for as long as is necessary to achieve the appropriate purpose for which it was collected. Canadian law societies provide guidance for lawyers regarding the ownership of a lawyer's file and the procedures that should be followed on closing a file, including retention considerations. To the extent that lawyers' files contain personal information, lawyers must reconcile their professional obligations with the requirements of PIPEDA. For example, PIPEDA requires organizations to retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected, used or disclosed. That requirement might suggest that personal information should be destroyed or anonymized when a lawyer's file is closed. However, lawyers must ensure that they retain any information that could be needed for the purposes of defending against any future allegations of negligence, misconduct or an assessment or review of the file. For such purposes, lawyers should nonetheless limit their retention of personal information to only the minimum needed. Following the expiration of any limitation period applicable to such claims, lawyers should destroy or de-identify the information.

In preparing their retention policies, lawyers are also strongly encouraged to plan responsibly for the proper transfer and storage of client files upon retirement, death, relocation, or in any situation they otherwise cease to practice law.

## Data breaches

Risk of data breaches can be prevented or significantly reduced through sound offline and online security safeguards, privacy policies and practices, and employee training. Data breaches can also be prevented or minimized by avoiding or limiting the collection of personal information in the first place. Lawyers should always consider whether they need to collect and retain personal information

at all. Such is not only a requirement of PIPEDA but also a sound management practice that can minimize the likelihood or scope of a data breach.

Although technical measures are an important component of security safeguards, administrative and organizational measures are equally important. Data breaches frequently occur because of carelessness or ignorance. In a busy legal practice where individuals are often working under tight timelines and in stressful situations, it is important for lawyers to anticipate potential mistakes and put in place measures to mitigate the risk of a data breach. Examples include: faxing, mailing or emailing personal information to the wrong recipient; taking home work on evenings or the weekends and losing personal information or having it stolen; leaving detailed personal information in voicemails destined for clients but accessible by others; falling prey to pretexters pretending to be someone they are not in order to get unauthorized access to client information; or making the grave mistake of opening suspect emails and attachments and rendering the entire office server vulnerable to hackers or identity thieves.

In order to avoid such careless or inadvertent disclosures of information, lawyers must establish and implement policies and procedures with an emphasis on ongoing employee testing and training. Such policies and procedures should include provisions to address communications with clients and others, confidentiality obligations, as well as authentication and identification procedures.<sup>10</sup> Employees should sign off on confidentiality agreements and acknowledge that they have been trained on privacy issues. Many organizations handling sensitive personal information train and test employees on privacy issues on an annual basis, and maintain a record of such activities. Lawyers should consider similar procedures.

If a data breach does occur, lawyers should immediately follow the following four steps:

- Step 1: Contain the breach and conduct a preliminary assessment;
- Step 2: Evaluate the risks associated with the breach, including consideration of the personal information involved, the cause and extent of the breach, how many individuals are affected, and the likelihood and type of harm that could occur;
- Step 3: Consider whether and how to notify any or all of the following: the affected individuals or clients, the Commissioner, the police, insurers, the law society or others; and
- Step 4: Prevent future breaches by learning from the incident and conducting any audit or other investigation that may be needed to address any systemic issues that resulted in the breach.<sup>11</sup>

The Commissioner strongly recommends that organizations subject to PIPEDA follow the above steps as a sound business measure. Organizations can report breaches to the Commissioner's Office in a variety of ways, including by phone, by e-mail and by regular mail.<sup>12</sup>

Lawyers should note that breach notification is mandatory in a number of other jurisdictions, such as Alberta, and Ontario in respect of personal health information.

## Employee personal information

PIPEDA does not apply to the personal information of employees except in respect of federally-regulated organizations, including any organization operating in one of the three territories. However, lawyers and law firms may be subject to provincial privacy legislation in this regard. Even in the absence of any applicable statute, however, lawyers and law firms should nonetheless protect the personal information of employees, and can take

guidance from a number of the findings involving federally-regulated organizations under PIPEDA.

For example, the surveillance of employees raises unique considerations and has been the subject of a number of Commissioner and court findings.<sup>13</sup> An organization should have evidence that the relationship of trust has been broken before conducting covert video surveillance. Mere suspicion is insufficient.

## International issues

When working on client or firm matters with an international dimension, lawyers must consider whether PIPEDA may apply to different aspects of each matter. PIPEDA was not intended to apply extra-territorially. However, the Commissioner has jurisdiction to investigate complaints relating to the trans-border flow of personal information. PIPEDA may apply to foreign entities that either receive or transmit communications to and from Canada, or that collect and disclose personal information about individuals in Canada. If there is a real and substantial connection to Canada, PIPEDA may apply to the activity.<sup>14</sup>

Other sections of this handbook touch on the requirements facing organizations, including lawyers and law firms, when they use foreign-based service providers to process information. The need to give notice to individuals and to use contractual and other means to ensure a comparable level of protection applies in all situations where lawyers may outsource aspects of their business to a service provider. This is an area of increasing relevance to lawyers and their clients. In some cases, foreign-based service providers now conduct document review and coding for relevance during litigation discovery. Contractual or other protections must be implemented. Best practices dictate that such

providers should be subject to strict contractual obligations and that they should only be able to access the information remotely from their country. Lawyers should also consider advising their clients of their outsourcing practices and any risks involved, as it is the client who may bear ultimate responsibility under PIPEDA to the individuals whose personal information is transferred to the service provider.

Lawyers crossing international borders should also be aware that any documents or devices they transport may be subject to a search by customs officials. For example, laptops, thumb drives, smart phones and other media could be subject to search by domestic and foreign border officials. Lawyers should consider such possibilities when determining how best to meet their obligations under PIPEDA, including properly safeguarding personal information.<sup>15</sup>

# PRIVACY ISSUES IN CIVIL LITIGATION

## Application of PIPEDA to litigation

Unlike the private-sector privacy laws in force in British Columbia and Alberta, PIPEDA does not contain a general exemption in respect of personal information available by law to a party in a legal proceeding. It does, however, contain several exceptions permitting the non-consensual collection, use or disclosure of personal information as may apply in the context of litigation proceedings (discussed below). PIPEDA thereby aims to ensure that organizations engaged in litigation are not unduly restricted in collecting, using or disclosing personal information where doing so is appropriate and necessary.

PIPEDA applies to organizations in respect of personal information collected, used and disclosed in the course of commercial activities. Is civil litigation a “commercial activity” for the purpose of PIPEDA? In an early case, the Ontario Superior Court commented, in *obiter*, that PIPEDA does not apply to an individual litigant who collects information about an opposing party through a private investigator.<sup>16</sup> In the Court’s view, PIPEDA would not have applied in that case since the defendant was collecting information for a purely personal purpose, namely, to defend himself in a lawsuit, notwithstanding that he had hired a private investigator to collect the information in question.

More recently, the Federal Court held that the collection of personal information about a plaintiff by an insurance company acting as agent for an individual defendant in a personal injury claim does not occur in the course of a commercial activity under PIPEDA.<sup>17</sup>

However, in light of the specific fact scenarios on which the above decisions are based, they should not necessarily be viewed as authority for the proposition that PIPEDA does not apply to any litigation at all. PIPEDA may continue to apply to aspects of litigation proceedings depending on the context. For example, the collection, use or disclosure of personal information in connection with litigation involving commercial organizations may well be carried out in the course of commercial activities, as distinguished from a personal injury claim involving individual litigants in their personal capacity.

Lawyers should therefore continue to be mindful of their PIPEDA obligations, and those of their clients. Lawyers should focus their efforts on ensuring that any personal information collected, used or disclosed in connection with any reasonably anticipated or actual litigation is done with either the express or implied consent of the individuals concerned, or otherwise meets one of the applicable exceptions to the knowledge and consent principles of the Act.

If personal information is collected, used or disclosed in litigation in contravention of PIPEDA, an individual could file a complaint to the Commissioner, or the Commissioner could herself initiate a complaint if she is satisfied there are reasonable grounds to do so. Ultimately, the matter could result in a hearing before the Federal Court. While a violation of PIPEDA during litigation will not necessarily render information inadmissible in civil litigation,<sup>18</sup> disregarding individual privacy can be a factor considered by the courts in awarding costs and in determining whether to remove counsel from the record.<sup>19</sup>

## Express consent, implied consent and exceptions to consent

Individual knowledge and consent is the cornerstone of PIPEDA. Express or implied consent, or a prescribed exception to the consent requirement, must always be present in respect of any collection, use or disclosure of personal information.

### Express consent

In the litigation context, obtaining express consent is often impractical or inappropriate, particularly when collecting information about an opposing party for the purpose of advancing a party's case. However, express consent should be obtained when seeking disclosure of personal information from a non-party to litigation, unless an applicable exception under PIPEDA applies, such as the requirement to comply with a subpoena or court order.

### Implied consent

Implied consent is the most prevalent form of consent relied upon in the litigation context. Courts have held that a party initiating litigation necessarily gives implied consent to a certain amount of probing of their private affairs for the proper

determination of the litigation.<sup>20</sup> A number of the Commissioner's findings echo this principle.

Organizations may rely on implied consent for collection, use and disclosure of personal information in a wide range of litigation activities, including in the context of settlement negotiations in certain circumstances.<sup>21</sup>

Established litigation rules will govern the scope of the implied consent in most cases. Implied consent does not authorize the unlimited or otherwise inappropriate collection, use or disclosure of an individual's personal information. Rather, any implied consent is limited to what a reasonable person would deem appropriate and what is relevant to the merits of the case. It is also limited by the general parameters of the implied undertaking rule. However, organizations still need to be mindful of the other provisions of PIPEDA when relying on implied consent in the context of litigation.

### Exceptions to consent

In many litigation matters, neither express nor implied consent will be applicable. This can be so where affected individuals are not parties to the litigation (e.g. where a corporate litigant's employee or customer personal information is involved). In such cases, lawyers and their clients must determine whether an exception to the knowledge and consent principle listed under section 7 of PIPEDA applies.

The following are relevant PIPEDA sections that tend to arise in the litigation context:

- *Collection* without consent is permitted under paragraph 7(1)(b) where it is reasonable to expect that:
  - the collection with the knowledge and consent of the individual would compromise the availability or 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, including the common law.
- *Use without consent* is permitted under paragraph 7(2)(d) where the information was collected under paragraph 7(1)(b) above; and
- *Disclosure without consent* is permitted by one of the exceptions listed under subsection 7(3), including the following:
  - for the purpose of collecting a debt owed by the individual;
  - where required to comply with a subpoena, warrant or order, or to comply with rules of court relating to the production of records; or,
  - when made to an investigative body on reasonable grounds to believe that the personal information relates to a breach of an agreement or a contravention of the laws of Canada or of a province or a foreign jurisdiction.

PIPEDA also permits the non-consensual collection, use or disclosure of certain publicly available information as prescribed in the regulations. However, just because information is in the public domain, for example, on a website or in a court file, does not mean that the information will be considered “publicly available” within the meaning of PIPEDA.

To be exempted from consent requirements for collection, use and disclosure, “publicly available information” must fall within one of the prescribed classes set out in the regulations (e.g. telephone books, professional or business directories, statutorily-created registries to which the right of public access is authorized by law, or documents of a judicial or quasi-judicial body that are available to the public) *and* the collection, use or disclosure must relate directly to the purpose for which the personal information appears in the public record,

document or registry. That said, even if personal information is “publicly available” within the meaning of the regulations and thereby exempted from consent requirements, it still must be protected by the other data protection principles of PIPEDA. For example, the collection, use, retention or disclosure of such information should be limited to only that which is necessary for fulfillment of the purposes identified.

### **Privacy issues arising in preparation for litigation**

Prior to the commencement of litigation, prospective parties and their lawyers will often collect, use and disclose personal information in the course of preparing for the litigation.

Until a claim is actually filed and defended, parties to a potential future claim cannot be said to have implicitly consented to certain litigation-related activities in respect of their personal information. Unless consent has been obtained by other means (e.g. the individual and the organization are in a contractual relationship which contains a clause that permits the collection, use or disclosure of the information if a dispute arises), the organization must look to one of the consent exceptions listed under section 7 of PIPEDA to verify whether the purported collection, use or disclosure is permissible.

### **Credit checks**

One pre-litigation issue that raises serious privacy concerns is the practice of conducting credit checks on an individual, more specifically, on a potential client or defendant. Such checks are usually done with a view to assessing a potential client’s ability to fund a litigation matter and effectively pay their bills, or a potential defendant’s solvency and resulting likelihood of collecting any monetary judgment. To the extent that the credit check is

conducted in the course of a commercial activity, for example to advance the business interests of the law firm or its corporate clients, then PIPEDA will generally prohibit such credit checks without the individual's consent, unless a relevant exception under section 7 of PIPEDA applies.

## Surveillance

Surveillance and similar forms of investigation are another common area of pre-litigation activity involving the collection, use and disclosure of personal information. Lawyers are often called upon to direct and/or provide advice regarding such pre-litigation surveillance and investigations.

Organizations that conduct surveillance directly or through a private investigator prior to the commencement of litigation must be alive to the requirements of PIPEDA. Organizations cannot collect personal information by way of surreptitious surveillance unless one of the enumerated exceptions to obtaining knowledge and consent under subsection 7(1) of the Act apply.

In assessing whether a reasonable person would find an organization's purposes for surveillance and recording of personal information to be appropriate under subsection 5(3) of PIPEDA, the Federal Court has applied the following test:

- Is surveillance and recording demonstrably necessary to meet a specific need?
- Is surveillance and recording likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?<sup>22</sup>

Building on the above test, organizations should limit both the type and amount of information

to that which is necessary to fulfill the identified purposes, including by limiting the duration and scope of the surveillance.

In addition, organizations should limit the collection of personal information about third parties who are not the subject of an investigation by selectively avoiding to record their images or any other personal information about them in the first place. If any such personal information is inadvertently or unavoidably collected, the organization should destroy or depersonalize it through blurring technology or other means as soon as is practicable.<sup>23</sup>

Organizations should document every decision to undertake surveillance and keep a record of its progress and outcome, ideally in conjunction with a formal surveillance policy.<sup>24</sup> In order to help ensure that organizations take into account all relevant considerations in determining whether and how to conduct surveillance activities, each of the factors described above should be reflected in written documentation. These considerations are relevant for surveillance activities instigated by lawyers or law firms themselves as organizations that may be subject to PIPEDA. They are also relevant to any advice lawyers or law firms dispense to their client organizations or any actions they undertake on their behalf in conducting surveillance in the course of commercial activity to which PIPEDA applies.

## Hiring a private investigator

Organizations, including lawyers, looking to hire a private investigator in connection with potential litigation or for other purposes should put in place a written agreement with the investigator, including explicit provisions to address privacy issues. It is the responsibility of both the investigator and the organization (often on the advice of its lawyer) to ensure that the investigation is conducted in

compliance with PIPEDA whenever it applies. The written agreement with the investigator should include the following provisions, among others:

- confirmation by the private investigator that it will collect personal information in a manner consistent with all applicable legislation, including PIPEDA;
- an acknowledgement by the hiring organization that it has authority under PIPEDA to collect from and disclose to the private investigator the personal information of the individual under investigation;
- a clear description of the purpose of the surveillance and the type of information sought;
- a requirement that the collection of personal information be limited; and
- a requirement that the collection of irrelevant information about third parties be avoided.<sup>25</sup>

## Pleadings

The culmination of a party's pre-litigation activities is often the drafting and delivery of a pleading, usually a statement of claim. Although it is widely accepted in practice that a party may disclose material personal information in a pleading without obtaining the consent of the affected individual(s), as a best practice, lawyers should ensure that disclosure of personal information in a pleading is kept to a minimum. Irrelevant or immaterial personal information should not be contained in a pleading.

## Privacy issues arising in the course of litigation

Litigation rarely proceeds in a predictable manner. Many of the pre-litigation issues identified in the preceding section of this handbook can and do arise after litigation has been commenced. Investigations can continue throughout the litigation process. Legal and factual issues can be added or removed from

litigation as it evolves, making it necessary to collect more personal information or, conversely, remove personal information in respect of questions no longer in issue. Lawyers must be vigilant in protecting privacy and in monitoring both their own and their clients' personal information management practices at each stage of an evolving litigation matter.

This section of the handbook is focused on privacy-related issues in the conduct of litigation, particularly discovery (including e-discovery and discovery of non-parties) and requests for access to personal information. Among other issues that may implicate PIPEDA, lawyers must consider the scope of what should be preserved and produced in discovery (e.g. whether entire hard drives and backup tapes need to be produced), the redaction of irrelevant personal information from otherwise relevant documents, and the location where documents can be reviewed by an opponent.

## The deemed undertaking rule

Before turning to the requirements of PIPEDA, it is important to note that courts have protected privacy interests in a variety of ways through rules of civil procedure and other means. For example, the deemed undertaking rule has long protected privacy interests in litigation. The concept of an implied undertaking or deemed undertaking exists in every Canadian jurisdiction, including the province of Quebec. The rule provides that "whatever is disclosed in the discovery room stays in the discovery room unless eventually revealed in the courtroom or disclosed by judicial order."<sup>26</sup> Information obtained on discovery may not be used for purposes collateral or ulterior to the proceedings in which it is disclosed. The primary rationale underlying the rule is the protection of privacy.

The deemed undertaking rule complements the PIPEDA principles that organizations may collect, use or disclose personal information only for purposes that a reasonable person would consider

appropriate in the circumstances, and must not use or disclose personal information for purposes other than those for which it was collected.

Moreover, in cases involving particularly sensitive personal information, parties have the option of protecting such information by seeking an order sealing the court file, naming the parties using their initials only, or protecting sensitive information by other available court orders.

### Relevance and proportionality

Principles of relevancy and proportionality can protect individual privacy because they limit the scope of information that must be disclosed in the discovery process. If personal information is not relevant to the litigation, it should not be collected, used or disclosed. As described earlier in this handbook, relevancy can also limit the scope of implied consent available to a party collecting information about an opponent in litigation. In other words, a litigant's implied consent to the collection, use or disclosure of their personal information will only extend to information that is relevant to the litigation.

Furthermore, the proportionality principle in litigation provides that diminishment of privacy is one of the non-monetary costs that should be considered in determining whether to preserve, produce or disclose documents in litigation. Although proportionality has arguably always been a part of the Canadian litigation landscape,<sup>27</sup> it has recently been formalized in respect of electronic discovery in the *Sedona Canada Principles for Electronic Discovery*.<sup>28</sup> Principle 2 provides that:

[...] the parties should ensure that steps taken in the discovery process are proportionate, taking into account (i) the nature and scope of the litigation, including the importance and complexity of the issues, interest and amounts at stake; (ii) the relevance of the electronically-stored information that is available; (iii) its importance to the court's adjudication in a given

case; and (iv) the costs, burden and delay that may be imposed on the parties to deal with electronically-stored information.

The commentary to Principle 2 confirms that privacy is one of the costs to dealing with electronically-stored information that must be taken into account by the parties to litigation. Lawyers should consider how relevance and proportionality may reduce or eliminate the need for their clients to demand or disclose personal information in litigation.

### Agreements and court directions to protect privacy

Principle 9 of the *Sedona Canada Principles* suggests that parties should agree to or seek court direction to protect privacy during e-discovery. As mentioned above, such protection might take the form of a sealing order, whereby the Court could order that all or part of the evidentiary record is to remain confidential. However, there are other areas where judicial direction may be needed. For example, parties may need to seek direction regarding the redaction of personal information from documents that are otherwise relevant to the litigation, or an order requiring an opposing party to keep in Canada any documents disclosed in discovery that contain personal information.<sup>29</sup> Short of seeking judicial direction regarding such matters, lawyers should try to anticipate and address privacy issues by agreement, including through participation in a meet-and-confer session.

### Privacy in electronic discovery

As the *Sedona Canada Principles* highlight, lawyers and clients need to be particularly sensitive to the requirements of PIPEDA in electronic discovery. In many cases, electronic devices such as computers and smart phones will contain a great deal of highly sensitive personal information about a number of individuals that is not relevant to the litigation. Individuals frequently use such devices

for employment or business purposes, and also for personal purposes, which routinely gives rise to privacy issues in litigation.

Courts have repeatedly rejected requests for production of entire hard drives and other electronic information on grounds that such production constitutes an unjustified invasion of privacy.<sup>30</sup> Even where production is ordered, courts will often impose privacy-protective measures to ensure that the invasion of privacy is kept to a minimum. For example, the court might instruct an independent expert to review the device for relevant information.<sup>31</sup>

Lawyers and clients that hire service providers to assist in managing electronic discovery issues should satisfy themselves that the service provider will comply with PIPEDA standards. The use of service providers is addressed in other sections of this handbook. The lawyer or the client must use contractual or other means to ensure that the personal information receives a comparable level of protection while being processed by the service provider. Service providers should always be asked whether they process or store any information outside of Canada. The Commissioner recommends that organizations give notice to individuals whose information is processed by a service provider outside of Canada. That recommendation may be difficult to apply in some litigation matters where notice may not be feasible, particularly in respect of personal information received from an opposing party in discovery.

### **Discovery of non-parties**

Organizations and their lawyers often look to non-party sources of information in litigation. Discovery of non-parties is often available under rules of civil procedure and through Norwich orders. The latter allows victims of alleged fraud to access potentially relevant information from third parties such as financial institutions.<sup>32</sup> Non-parties such as Internet

service providers, telecommunication service providers, social media providers, banks, hospitals and others hold a great deal of information about individuals' day-to-day activities. This information can be extremely valuable in litigation but must be obtained in compliance with PIPEDA.

Absent exceptional circumstances such as a threat to health or safety, non-parties should not agree to disclose personal information to litigants or potential litigants without consent or a court order.<sup>33</sup> A summons to witness may qualify as a court order but no information should be disclosed unless specifically provided for in the summons.<sup>34</sup> For example, if a summons requires a witness to attend court to give evidence and to bring relevant documents, documents containing personal information should not be disclosed to the requesting party in advance of the appearance, unless the consent of the individual is otherwise obtained.

Compliance with PIPEDA in this context requires that the personal information to be disclosed must be relevant and limited to that which is necessary to fulfill the purpose. Disclosure must only be made to the organization named in the order. As a best practice, lawyers should always consider whether there may be alternative ways to obtain the information sought, including by less privacy-invasive means. Such alternatives should be exhausted before requesting information from a non-party. Courts may refuse to compel disclosure from a non-party where alternative means exist to obtain the information.<sup>35</sup>

Lawyers must also be alert to the fact that a court may refuse to order a non-party to disclose personal information if the materials in support of the motion demonstrate that the requesting party has unduly infringed on the affected individual's privacy interests.<sup>36</sup>

## Access requests and litigation

### Access requests under PIPEDA

In the course of a litigation matter and in some cases before litigation, lawyers and their clients may receive requests for access to personal information from an actual or potential opposing party or other individuals, including witnesses.

Notwithstanding that a litigation proceeding may be underway, all organizations must respond to access requests in accordance with PIPEDA.<sup>37</sup> Access may be legitimately refused under PIPEDA on grounds that the information is subject to solicitor-client privilege (which includes both legal advice and litigation privilege),<sup>38</sup> or generated in the course of a formal dispute resolution process. However, access may not be refused merely because there are parallel litigation proceedings underway that may involve some of the same information. An individual's right of access is a fundamental right, untempered by that individual's motive for seeking access.

Lawyers should also be aware that where access to personal information is refused and the individual subsequently files a complaint with the Commissioner, the Commissioner is not required to investigate the complaint in every case. The Commissioner may decline to investigate if she is satisfied that the access request could more appropriately be dealt with, initially or completely through the procedures available to the parties in the parallel litigation process.<sup>39</sup> For example, where the sole issue in the complaint is whether the information being sought is litigation-privileged, the Commissioner may direct the parties to seek resolution of the issue before the courts as part of the ongoing litigation matter.<sup>40</sup>

### Claims of solicitor-client privilege under PIPEDA

The Commissioner has the duty to investigate complaints relating to violations of PIPEDA, including complaints against an organization for refusal to provide access to personal information upon request. During the course of her investigation, the Commissioner has broad powers to ensure she can effectively and meaningfully investigate such complaints. However, the courts have recently clarified that the Commissioner may not compel the production of information over which an organization claims solicitor-client privilege, or otherwise compel organizations to produce a justification for their claim by way of affidavit for example.

Nevertheless, and unless the Commissioner exercises her discretion to decline to investigate a complaint in applicable circumstances, the Commissioner must still investigate and report on complaints relating to refusal of access on grounds of solicitor-client privilege. In order to carry out her mandate, the Commissioner may accept evidence voluntarily tendered by the organization to support its claim. Alternatively, she may refer the matter to the Federal Court under section 18.3 of the *Federal Courts Act*, or she may declare an impasse and proceed to file an application for a court hearing before the Federal Court under section 15 of PIPEDA.

Organizations, including lawyers, should seriously gauge whether personal information they are refusing to release to an individual is indeed solicitor-client privileged, and in cases involving claims of litigation privilege, whether the personal information being sought was created for the dominant purpose of actual or reasonably anticipated litigation and whether such privilege has since expired.

# CONCLUSION

As described in this handbook, lawyers are often entrusted with sensitive personal information about their clients and other individuals. Although lawyers have long been subject to legal and professional responsibilities regarding their collection, use and disclosure of such information, lawyers must also carefully consider their compliance with privacy laws, including PIPEDA where applicable.

In some cases, the requirements of PIPEDA mirror lawyers' existing professional requirements. In other cases, navigating the requirements of PIPEDA in a legal practice can add further complexity. Lawyers must not only consider their own privacy obligations but also the different obligations that each of their clients may face. Privacy obligations applicable to clients can sometimes restrict what lawyers can do with personal information they collect, use or disclose on their clients' behalf. It is hoped that this handbook will assist lawyers in identifying and complying with various PIPEDA requirements that apply in the day-to-day management of a law practice and in the context of civil litigation. In addition to this handbook, lawyers are encouraged to consult PIPEDA and other additional resources, including the material published by the Commissioner at [www.priv.gc.ca](http://www.priv.gc.ca).

The Commissioner's website is updated frequently and contains a wide range of links and additional resources that expand on a number of the issues highlighted in this handbook, including:

- summaries of key findings interpreting the provisions of PIPEDA;
- guidelines on surveillance, data breaches and other topics;
- tools, tips, checklists and questionnaires to help facilitate organizations' compliance with PIPEDA;
- interpretation bulletins that address key provisions in PIPEDA such as the definitions of "personal information" and "commercial activity"; and
- reports of public consultations and other initiatives undertaken by the Commissioner.

There are also an increasing number of court decisions that address different aspects of PIPEDA. Lawyers are encouraged to stay abreast of relevant developments to ensure ongoing compliance with PIPEDA, and most importantly, to serve as exemplary models of ethical and respectful conduct on behalf of the profession and the clients they serve.

# ENDNOTES

- 1 Canada (*Information Commissioner*) v. Canada (*Transportation Accident Investigation and Safety Board*), 2006 FCA 157; Dagg v. Canada (Minister of Finance), [1997] 2 S.C.R. 403.
- 2 *Gordon v. Canada (Health)*, 2008 FC 258.
- 3 *Wyndowe v. Rousseau*, 2008 FCA 39.
- 4 See e.g. PIPEDA Case Summary #2007-377: Law firm's shoddy privacy practices result in missing personal information; request for access denied; PIPEDA Case Summary #2006-340: Law firms collected credit reports without consent; and PIPEDA Settled Case Summary #30: Solicitor's lien insufficient grounds to deny access to personal information.
- 5 PIPEDA Case Summary #2007-377 - Law firm's shoddy privacy practices result in missing personal information; request for access denied.
- 6 See e.g. PIPEDA Case Summary #192 - Bank does not obtain the meaningful consent of customers for disclosure of personal information.
- 7 PIPEDA Settled Case Summary #30: Solicitor's lien insufficient grounds to deny access to personal information.
- 8 See e.g. PIPEDA Case Summary #2008-394 - Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers.
- 9 See the Commissioner's tool entitled *Securing Personal Information: A Self-Assessment Tool for Organizations*, available at: <http://www.priv.gc.ca/resource/tool-outil/security-secureite/english/AssessRisks.asp?x=1>
- 10 See e.g. Guidelines for Identification and Authentication, available at: [http://www.priv.gc.ca/information/guide/auth\\_061013\\_e.cfm](http://www.priv.gc.ca/information/guide/auth_061013_e.cfm)
- 11 These steps are based on the Commissioner's publication titled *Key Steps for Organizations in Responding to Privacy Breaches*, available at: [http://www.priv.gc.ca/information/guide/2007/gl\\_070801\\_02\\_e.cfm](http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.cfm)
- 12 For further information on reporting data breaches, including accessing the Office's Privacy Breach Incident Report Form, see [http://www.priv.gc.ca/resource/pb-avp/pb\\_form\\_e.cfm#contenttop](http://www.priv.gc.ca/resource/pb-avp/pb_form_e.cfm#contenttop)
- 13 See *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act*, [http://www.priv.gc.ca/information/pub/lbe\\_080523\\_e.cfm](http://www.priv.gc.ca/information/pub/lbe_080523_e.cfm)
- 14 See e.g. *Lawson v. Accusearch Inc.*, 2007 FC 125.
- 15 For suggested best practices, see the Canadian Bar Association publication "How to Secure Your Laptop Before Crossing the Border" available at <http://www.cba.org/cba/practicelink/tayp/laptopborder.aspx>
- 16 *Ferency v. MCI Medical Clinics*, 2004 CanLII 12555 (ON SC).
- 17 *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*, 2010 FC 736.
- 18 *Ferency v. MCI Medical Clinics*, 2004 CanLII 12555 (ON SC); see also PIPEDA Case Summary #2005-311: A Woman's Activities Recorded and Videotaped by a Private Investigator Hired by an Insurance Company.

- 19 See e.g. *Osiris Inc. v. 1444707 Ontario Ltd.*, 2005 CanLII 47731 (ON SC).
- 20 See e.g. *M. (A.) v. Ryan*, [1997] 1 S.C.R. 157.
- 21 See e.g. PIPEDA Case Summary #2006-331: Credit card account history disclosed to estranged spouse.
- 22 *Eastmond v. Canadian Pacific Railway*, 2004 FC 852.
- 23 PIPEDA Case summary #2009-007: Mother and daughter were videotaped during covert surveillance of another individual.
- 24 *Guidance on Covert Video Surveillance in the Private Sector* - [http://www.priv.gc.ca/information/pub/gd\\_cvs\\_20090527\\_e.cfm](http://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.cfm) and *Guidelines for Overt Video Surveillance in the Private Sector* - [http://www.priv.gc.ca/information/guide/2008/gl\\_vs\\_080306\\_e.cfm](http://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.cfm)
- 25 *Ibid.*
- 26 *Juman v. Doucette*, 2008 SCC 8 at para. 25.
- 27 See e.g. *Peter Kiewit Sons Co. of Canada Ltd. v. British Columbia Hydro & Power Authority* (1982), 36 BCLR 58 (S.) at paras. 22-23.
- 28 Available at <http://www.lexum.com/e-discovery/documents/SedonaCanadaPrinciples01-08.pdf>
- 29 See e.g. *DataTreasury Corporation v. Royal Bank of Canada*, 2008 FC 955.
- 30 See e.g. *Desgagne v. Yuen*, 2006 BCSC 955; *Baldwin Janzen Insurance Services (2004) Ltd. (c.o.b. Baldwin Insurance Brokers) v. Janzen*, [2006] B.C.J. No. 753 (S.C.).
- 31 *Vector Transportation Services Inc. v. Traffic Tech Inc.*, 2008 CanLII 11050 (ON SC).
- 32 See generally *GEA Group AG v. Ventra Group Co.*, 2009 ONCA 619; *Alberta (Treasury Branches) v. Leahy* (2000), 270 A.R. 1 (Q.B.), *aff'd* (2002), 303 A.R. 63 (C.A.), leave to appeal refused [2002] S.C.C.A. No. 235.
- 33 *BMG Canada Inc. v. Doe*, 2005 FCA 193.
- 34 PIPEDA Case Summary #2009-005: Husband's financial information disclosed to wife's lawyers by accounting firm improperly complying with Summons to Witness.
- 35 See e.g. *Citi Cards Canada Inc. v. Pleasance*, 2011 ONCA 3.
- 36 *BMG v. Doe*, *supra* note 31.
- 37 PIPEDA Case Summary #352 - Airline delays granting access to personal information, citing ongoing litigation.
- 38 *Blank v. Canada (Minister of Justice)*, 2006 SCC 39.
- 39 PIPEDA, s. 12(1)(b).
- 40 PIPEDA Case Summary #2010-011 - Commissioner does not issue report to individual seeking access to her personal information being withheld for reasons of solicitor-client privilege.



Office of the  
Privacy Commissioner  
of Canada

**For more information**

For general inquiries please visit our website at  
**[www.priv.gc.ca](http://www.priv.gc.ca)** or call us:

Toll-free: 1-800-282-1376

Tel: 613-947-1698

TTY/TDD: 613-992-9190

Fax: 613-947-6850

Follow us on Twitter: @PrivacyPrivee

Cat. No.: IP54-40/2011E-PDF

ISBN: 978-1-100-53540-1