



THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

***Personal Information Protection
and Electronic Documents Act
(PIPEDA)***

**NATIONAL PRIVACY AND ACCESS LAW SECTION
CANADIAN BAR ASSOCIATION**

January 2008

TABLE OF CONTENTS

Personal Information Protection and Electronic Documents Act (PIPEDA)

| | | |
|-------------|--|-----------|
| I. | INTRODUCTION | 1 |
| II. | DATA BREACH NOTIFICATION | 2 |
| | A. Context | 2 |
| | B. Analysis | 4 |
| | Criteria for Notification/Reporting..... | 4 |
| | Content of Reports to Commissioner..... | 7 |
| | Penalties | 8 |
| | Ability of the Commissioner to Make Information Public..... | 8 |
| | Other Elements – Timing and Notification of Credit Bureaus | 9 |
| III. | WORK PRODUCT | 10 |
| | A. Is an Amendment Needed?..... | 10 |
| | B. Implementation Issues..... | 12 |
| IV. | LAWFUL AUTHORITY | 13 |
| | A. Current Uncertainty..... | 13 |
| | B. Recent Clarification..... | 14 |
| | C. Options for Further Clarification..... | 15 |
| V. | INVESTIGATIONS AND INVESTIGATIVE BODIES | 16 |
| VI. | PARTS (PRIVACY AWARENESS RAISING TOOLS) | 17 |

| | | |
|--------------|--|-----------|
| VII. | IMPACT ON THE LITIGATION PROCESS | 18 |
| | A. Investigations and Witness Statements | 18 |
| | B. Other Effects on the Litigation Process | 19 |
| VIII. | CONCLUSION..... | 23 |

PREFACE

The Canadian Bar Association is a national association representing 37,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the National Privacy and Access Law Section of the Canadian Bar Association, with assistance from the Legislation and Law Reform Directorate at the National Office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the National Privacy and Access Law Section of the Canadian Bar Association.

Personal Information Protection and Electronic Documents Act (PIPEDA)

I. INTRODUCTION

The Canadian Bar Association National Privacy and Access Law Section (CBA Section) is pleased to respond to Industry Canada's consultation on the Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics on the *Personal Information Protection and Electronic Documents Act* (PIPEDA).¹

The CBA Section has previously provided comments and recommendations respecting the statutory review of PIPEDA to Industry Canada, the Privacy Commissioner of Canada (the Commissioner) and the Standing Committee.² Many of our comments and recommendations for legislative change were accepted by the Standing Committee and also supported in the Government Response.

In this submission, the CBA Section focuses on the following issues:

- data breach notification;
- work product;
- lawful authority;
- investigations and investigative bodies;
- PIPEDA Awareness Raising Tools (PARTS); and
- neutrality in regard to the litigation process.

¹ Canada *Gazette* Notice October 27, 2007.

² National Privacy and Access Law Section, *Preparing for the 2006 Review of the Personal Information Protection and Electronic Documents Act* (Ottawa: CBA, 2005); *Preparing for the 2006 Review of the Personal Information Protection and Electronic Documents Act – Case Examples* (Ottawa: CBA, 2005); PIPEDA Review (Ottawa: CBA, 2006); Five year review of the *Personal Information Protection and Electronic Documents Act* (Ottawa: CBA, 2006).

II. DATA BREACH NOTIFICATION

A. Context

This section analyzes the parameters for notification of individuals and reporting breaches of personal information to the Commissioner, as well as other considerations for developing a breach notification model.

The Government addressed Recommendations 23, 24 and 25 of the Report in its Response.

To paraphrase:

- for a certain defined category of breaches where a high risk of significant harm exists, there should be a statutory requirement for prompt notification of individuals affected by the breach;
- there should be a statutory requirement to report any major loss or theft of personal information to the Privacy Commissioner within a specified period of time;
- the Privacy Commissioner should not act as a “gatekeeper” to decide which breaches are subject to a notification requirement; but instead that determination should be made by the organization involved, based on criteria set out in the legislation and/or guidelines; and
- consultation, research and analysis will be used to determine elements of the notification and reporting parameters including thresholds, timing, form and content, as well as requirements to notify other industry-related organizations.

The Commissioner strongly recommends amending the *Act* to include breach notification, but recognizes that finding the appropriate model will require time and consultation with stakeholders. Currently, only the *Ontario Personal Health Information Protection Act* (PHIPA) expressly requires that individuals be notified of any unauthorized collection, use or disclosure of personal information.

There are three general options with respect to breach notification in the normal spectrum of events. The first option would be to maintain the status quo, based on arguments that:

- PIPEDA already obliges organizations to safeguard personal information, and some interpret that as extending to notification when personal information has been lost, stolen or otherwise accessed without authorization;
- businesses already have incentives to notify when appropriate;

- imposing a duty to notify for every breach could desensitize consumers to notices; and
- businesses are well placed and require flexibility to assess the risk represented by each security breach.

At the other end of the spectrum would be the option of imposing an unqualified obligation on organizations to notify individuals in *all* cases of a breach. This is the approach adopted by PHIPA because of the inherent sensitivity of personal health information.³

An intermediate option would be a balanced approach requiring notification in some circumstances. In its 2005 submission, the CBA Section recommended this approach if a duty to notify was to be included in PIPEDA, and this recommendation was expressly recognized in the Standing Committee Report. The CBA Section referred to California's SB 1386, where a duty to notify is imposed if two thresholds are met:

- **Insufficient encryption:** The information is (a) unencrypted or otherwise unprotected so there is no reasonable assurance that the information is inaccessible, or (b) encrypted or otherwise so protected, but the organization has received notice that the protection has been breached; and
- **Information is sensitive:** The information falls in a specified category of types of sensitive personal information [e.g. Social Insurance Numbers, sensitive financial information (including bank account numbers, credit card numbers, and associated passwords and PINs) and health information].⁴

In its white paper on the issue,⁵ the Canadian Internet Policy and Public Interest Clinic recommended a similar balanced approach where notification would be required if “designated personal information” has been or is reasonably believed to have been acquired by an unauthorized person. The term “designated personal information” is defined to:

- include government issued ID numbers (SIN, drivers' licence numbers or health card numbers) and account numbers, credit or debit card numbers; and
- exclude information that is encrypted, redacted or otherwise altered by any method or technology in such a manner that the name/data elements are unreadable by unauthorized persons.

³ *Personal Health Information Protection Act*, SO 2004, c.3, s. 12(2).

⁴ National Privacy and Access Law Section, *supra* note 2 at 40.

⁵ *Approaches to Security Breach Notification* (January 2007) <http://www.cippic.ca/en/>.

While formulated somewhat differently, both approaches suggest notification criteria based on an assessment of *the potential risk of harm for the individual*, considering the sensitivity of the information in question and the probability that the information would be accessed.

In its response to Recommendation 23, the Government also enumerated purposes for which the Commissioner would receive reports of *a major loss or theft of personal information* (collectively, the “Reporting Purposes”):

- to allow for oversight of organizational practices
- to track the volume and nature of breaches
- to track the steps taken by organizations respecting the notification process when that process is required, and
- to assist small and medium-sized enterprises (SMEs), that may lack the internal resources necessary to make notification assessments regarding the notification process.

According to the Government Response, the imperative is for notification to take place promptly and for reporting to occur within a specified time frame. We note that notification and reporting are distinct functions, and the timing of each may or may not be related, depending on the facts. Usually, notification would occur at the earliest opportunity while reporting may (and often will likely) occur later, after more information is known and steps have been taken by the organization to ensure the report is meaningful. However, as is currently the case, a report can be made to the Commissioner before notification if an organization seeks guidance on whether to notify, or wants to promptly alert the Commissioner to the breach. Similarly, any organization could seek guidance without making a formal report and if required to report, could do so later.

B. Analysis

Criteria for Notification/Reporting

The Government Response effectively recommends a dual obligation model. Organizations determine the need for notification if there is a “high risk of significant harm” to individuals, and must report the breach to the Commissioner if the “major loss or theft” threshold is met.

Our analysis assumes that similar factors can be used to assess the severity of a breach based on either the “high risk” or “major loss” criterion. However, we recognize that any intended distinctions suggested by the different terminology must also be considered.

The possible relationships between the threshold for notification and the threshold for reporting are:

- The notification criteria could have a lower threshold than for reporting i.e. the severity of an incident that requires notification would be less than an incident that requires reporting. Depending on how the notification/reporting mechanism is structured, this would mean that not all incidents requiring notification would be reported to the Commissioner, as the organization could be obliged to notify individuals of a breach but not to report the breach.
- The notification criteria could have the same threshold as the reporting criteria: i.e. incidents would be of the same severity for both notification and reporting. In this case, all reportable incidents would require notification and all notified incidents would require reporting.
- The notification criteria could represent a higher threshold than the reporting criteria: i.e. the severity of an incident that requires notification would be higher than an incident that requires reporting. In other words, of the incidents that would be reported on the “major loss” criterion, only a smaller subset would require notification. All potentially notifiable breaches would be reported, as would other incidents that meet the major loss criterion.

To the extent that not all breaches or notifiable incidents are to be reported, the Reporting Purposes would not be satisfied in that the full extent or treatment of all breaches would not be known by the Commissioner. The general objectives of the Reporting Purposes must be read in the context of the express limitation of reporting where there is “major loss or theft”.

In regard to the Reporting Purpose of assisting SMEs with the notification process, we assume the intent is for the Commissioner to offer assistance and guidance to SMEs who voluntarily seek it, as is currently the case, and also to allow the Commissioner to benefit from data collected through all reports received.

The CBA Section has not critically evaluated the Reporting Purposes, but rather accepts them as representing the Government’s objectives in developing a reporting mechanism and offers comment and suggestions.

Whichever relationship model is adopted, the relevant criteria for the two separate activities must be determined. While the Government Response suggests that the notification criteria is based on an assessment of the high risk of harm to individuals, the question of how to assess the reporting threshold of a major loss or theft of personal information remains.

We considered the interaction of three factors in determining when notification or reporting would be required in various situations: i) number of individuals impacted; ii) sensitivity of information involved; and iii) probability that information was accessed. Of course, flexibility will be required in making any such determination. The following chart outlines anticipated outcomes based on the interplay of these factors:

| Number of individuals | Sensitivity of information | Probability of access | Reportable? | Notifiable? |
|-----------------------|----------------------------|-----------------------|-------------|-------------|
| Low | Low | Low | No | No |
| High | Low | Low | Possibly | No |
| Low | High | Low | Possibly | No |
| Low | Low | High | No | No |
| Low | High | High | Possibly | Yes |
| High | High | Low | Yes | No |
| High | Low | High | Yes | Possibly |
| High | High | High | Yes | Yes |

For example, if the information is sensitive but involves only a few individuals and the probability of access is high, the organization should be required to notify. However, the decision to report may depend on the particular circumstances of the breach. If, in the same situation, the probability of access is relatively low, reporting without notification may be sufficient, or neither may be required.

The number of individuals affected by a breach may also be a determining factor in whether to report a breach. Clearly, to meet the “major loss” threshold criterion, an incident where only a single individual is affected would likely not require reporting. However, if a pattern

of similar breaches of information occurred over a period of time, reporting may well be appropriate. For example, if the number of individuals affected is low, but the sensitivity and probability of access are both high, reporting might be required, particularly if there was a pattern of multiple incidents with similar characteristics that might indicate a systemic problem within the affected organization.

Generally:

- an organization would only report an incident (as a “major loss or theft of personal information”) if the sensitivity of the information is high. However, for policy reasons, an incident should perhaps be reported where the number of individuals is high and the probability of access is high, even though the information itself is of low sensitivity, as such an incident might qualify as a “major loss”; further, reporting might be appropriate where the number of individuals affected is high, even though the sensitivity and access factors are both low, simply given the number of people potentially impacted by the breach;
- an organization would only be obliged to notify (as a result of a “high risk of significant harm” to the individual) where the sensitivity of the information is high and the probability of access is high.⁶

Content of Reports to Commissioner

The CBA Section encourages an approach to reporting where the contents of a report to the Commissioner are based simply on facts. The BC Information and Privacy Commissioner’s *Privacy Breach Reporting Form (November 2006)* asks for general information about the facts of the breach. The same form also asks the organization to identify types of harm that may result from the breach, which is speculative and may actually discourage proactive reporting. In contrast, a factually based form will encourage reporting. In our view it should be developed by the Commissioner in collaboration with all stakeholders.

⁶ This is consistent with the approach recommended in our 2005 submission. See, *supra* note 2 at 40.

Penalties

Recommendation 25 of the Standing Committee Report suggests consideration be given to “penalties for failure to notify”, though the Government Response does not address that issue. This raises complex issues. For example, if the organization experiencing the breach is responsible for deciding when to notify, how would it be determined that the organization had come to the “wrong” decision, what standard would be used and how would an offence or penalty for failing to notify be levied? The existing offences and penalties in PIPEDA include a significant element of malfeasance, so a “wrong decision” about notification may not be appropriately egregious to warrant it being made an offence at a similar level as the offences currently found in PIPEDA.

The CBA Section does not support the suggestion in the Standing Committee Report⁷ that it be an offence under PIPEDA to fail to notify of a breach where a “reasonable person” would expect disclosure to have taken place. While there are references to the obligation to be reasonable throughout PIPEDA, none serve as the basis for an offence. It would again be inconsistent to introduce an offence based on a “reasonable person” test.

If potential penalties for failure to notify will be considered further in future, the CBA Section would be pleased to participate in that study.

Ability of the Commissioner to Make Information Public

Section 20 of PIPEDA obliges the Commissioner and agents of the Commissioner to preserve the confidentiality of information that comes to their knowledge as a result of the performance or exercise of any duties or powers under the *Act*. The section also sets out exceptions to this obligation. For example, the Commissioner can make any information relating to the personal information management practices of an organization public if the Commissioner considers that it is in the public interest to do so.

⁷

Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics on the *Personal Information Protection and Electronic Documents Act (PIPEDA)* at 43.

We suggest that the interaction between the responsibility of the affected organization to decide about notification, the new requirement for the organization to report to the Commissioner in certain cases and the Commissioner's existing power to make information public when in the public interest should be carefully considered. If the organization has decided that notification would be inappropriate in the circumstances, it could be problematic for it if the Commissioner subsequently decides to make the information public.

Other Elements – Timing and Notification of Credit Bureaus

The CBA Section agrees that notification of affected individuals should be prompt. However, we suggest that rather than a specific timeframe in the legislation, the timing of notification and reporting should be specified in regulations or guidelines to accommodate particular considerations and circumstances of each breach. For example, it may be necessary to delay notification taking into consideration law enforcement and other investigations, as has been suggested by the Commissioner in recent guidelines:

Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. However, if law enforcement authorities are involved, those authorities should be consulted as to whether notification should be delayed to ensure that the investigation is not compromised.⁸

A possible formulation of the rule might be:

Notification of affected individuals should be given at the earliest time taking into consideration risks of harm, the status of any investigations, the appropriate method of notification and other relevant factors.

Certainly the basic requirement for reporting should be set out in the legislation (e.g. “within a reasonable time”). However, guidelines developed by the Commissioner in collaboration with stakeholders would provide appropriate guidance on the expected time for reporting a breach. There should be no requirement that reporting occur prior to notification, although an organization could report as early as it deems appropriate. Given the Commissioner's oversight rather than gate keeping role, the time to report need also not be particularly short. We suggest that 45-90 days would be reasonable. This would allow the organization to complete its response to the breach and collect as many facts as possible to report to the

⁸ *Key Steps for Organizations in Responding to Privacy Breaches* (Ottawa: Office of the Privacy Commissioner of Canada, August 2007).

Commissioner. Again, nothing prevents an organization from reporting earlier and seeking guidance, whether or not statutorily required.

As with timing, the CBA Section believes that specific criteria regarding the form and mode of notification and reporting are best left to regulation or guidelines issued by the Commissioner. This approach allows for more specificity and flexibility to reflect different circumstances of each breach and allows rules to be modified to reflect future experience. The CBA Section is prepared to provide additional comments regarding these elements in any further consultation.

Consideration should be given to a power or even obligation to notify credit bureaus of potential fraud risks connected with a breach without consent. Credit bureaus and groups representing credit grantors should be consulted to understand the implications of allowing such notification. Credit bureaus represent the primary focus for credit grantors validating requests for credit or other financial commitments, such as insurance, and can usefully act as a first line of defence against potential identity fraud or theft. Again, the CBA Section would be prepared to consider further the issue of organizations that might also qualify for fraud prevention in any further consultation regarding the breach response process.

III. WORK PRODUCT

A. Is an Amendment Needed?

In 2005, the CBA Section recommended that PIPEDA be amended to provide for an explicit definition of “work product information” and that such information be excluded from the definition of “personal information” in the *Act*. We said:

The definition of “personal information” should be clarified to be consistent with both the Federal Commissioner’s finding in PIPEDA Case Summary #15 and the exclusion of “work product information” in the BC PIPA, which in effect codifies the Commissioner’s finding. Certainty as to the scope of PIPEDA is critical for business organizations to ensure that all information simply referring to an employee is not considered the personal information of that individual for the purposes of access. In addition, codification of this exclusion would recognize, as did the Federal Commissioner and the BC *Act*, that just because information “relates” to an individual, it is not necessarily “about” them in a personal sense.

This exclusion may be contrasted with the Assistant Commissioner's finding in PIPEDA Case Summary #303 that the number of houses sold by real estate agents in a year was their personal information. Not only is such information clearly "about" these individuals, it represents financial information about those agents' income. However, the finding in that case did not expressly distinguish the finding in Case Summary #15. This has generated some uncertainty about the "work product" exception set out in case Summary #15, an exception that has governed organizations' treatment of business records since the early days of PIPEDA's enactment. Amending PIPEDA to codify the "work product" distinction in Case Summary #15 would resolve this uncertainty, and also conform to the expressed policy intent of Industry Canada when the legislation was developed.⁹

In testifying before the Standing Committee in November 2006, the Commissioner stated:

We recognize that an individual in his or her capacity as an employee or as a professional may generate information that is not about the individual.¹⁰

The Commissioner and others that appeared before the Standing Committee seem to agree that there is a category of "work product information" which, while identified with an individual, should not be considered that individual's "personal information". However, the Commissioner has also cautioned that certain information collected in the course of managing a workplace might be deemed to be "work product" to avoid being considered the personal information of employees in the workplace (such as surveillance videos).

The CBA Section continues to believe that an amendment to PIPEDA is needed. In the absence of a specific definition in the *Act*, "work product information" could mean different things to different people. For example, individuals requesting access to their personal information from an organization might maintain that every memorandum letter they wrote as an employee was their personal information, and they should therefore receive access. On the other hand, the organization could take the position that these documents were "work product information" and that access was not required. Without the guidance of an actual definition, such cases could end up as complaints before the Commissioner, consuming time and resources more usefully directed elsewhere. Further, the absence of a definition leads to uncertainty for individuals as to their rights and for organizations as to their responsibilities. In our view, any concerns about unintended application of a "work product" exclusion could be addressed by appropriate definitions supplemented by ongoing legislative interpretation.

⁹ *Supra*, note 2 at 6-7.

¹⁰ <http://cmte.parl.gc.ca/cmte/CommitteePublication.aspx?SourceId=186780&Lang=1&PARLSES=391&JNT=0&COM=10473> at 1530.

The application of any legislation to the particular facts at hand will always involve legislative interpretation as to context. Interpretation is easiest when clear direction is provided in legislation. The amendment we propose below would enable this process to occur with greater certainty.

B. Implementation Issues

On the issue of defining work product, the Standing Committee agreed with the CBA Section that reference should be made to the definition in BC PIPA, but also recommended that consideration be given to the approach taken to professional information in Québec's legislation.¹¹

We disagree that the Québec approach is appropriate as a model for amending PIPEDA. Its scope is limited to the information of *professionals* regarding their professional activities, so it is not readily applicable to information related to other individuals prepared or collected as part of employment responsibilities. The component of the Québec law that mandates consultation with professional orders would be inappropriate or impossible for other categories of employees. From a process perspective, the Québec approach would demand significant resources of the Commissioner's office or any other body created to manage applications for the authorized use of "work product information". Finally, the "opt-out" provision of the Québec approach would be problematic, as it could lead to inconsistencies in how data is treated within an organization.

The CBA Section repeats that the definition of "work product information" in BC PIPA should be used to amend PIPEDA. That definition reads:

"work product information" means information prepared, compiled or disclosed by an individual or group as part of the individual or group's responsibilities related to their profession, employment or business. It does not include personal information about an identifiable individual who did not prepare, compile or disclose the information.¹²

¹¹ *An Act respecting the protection of personal information in the private sector*, RSQ, c. P-39.1.

¹² *Personal Information Protection Act (PIPA)*, SBC 2003, c.63.

To address the concerns expressed by the Commissioner and others about the risk of unintended consequences to employee privacy as a result of an exemption under PIPEDA, an additional exception could be added to the definition. The second sentence could instead read:

It does not include: (i) personal information about an identifiable individual who did not prepare, compile or disclose the information, or (ii) *information about employees collected, used or disclosed for the purposes of managing the workplace.*

IV. LAWFUL AUTHORITY

A. Current Uncertainty

PIPEDA provides a regime that governs the collection, use and disclosure of personal information by the private sector, and generally requires the knowledge and consent of the individual. PIPEDA also provides for specific circumstances where personal information can be collected, used and disclosed without consent. Section 7(3) outlines limited circumstances when organizations “may” disclose personal information without consent.

Little confusion has arisen about an organization’s ability to disclose when a warrant or court order is presented pursuant to section 7(3)(c) or when disclosure is required by law pursuant to section 7(3)(i). However, uncertainty and confusion does arise when the request is from a law enforcement agency (LEA), such as the RCMP or a provincial police force, as to what “lawful authority” pursuant to section 7(3)(c.1) means in that particular context. Some LEAs have even relied on this section of PIPEDA in their request for information as their actual “lawful authority” to obtain the requested information.¹³

¹³

This point was discussed in more detail in a recent CBA submission on the issue of law enforcement access to customer name address information (Ottawa: CBA, 2007).

B. Recent Clarification

During review of PIPEDA and a Public Safety Canada “lawful access” consultation last fall,¹⁴ this issue was discussed and some previous confusion may have been resolved. Law enforcement agencies increasingly appreciate that section 7(3)(c.1) of PIPEDA does not provide their lawful authority to obtain the requested information, but rather establishes a discretionary regime pursuant to which organizations *may* disclose personal information when the relevant requirements of the section in question have been met. Further, there is now clear language from both the Government and the Commissioner regarding the legislative intent of this provision.

The Government Response clearly states that:

The government wishes to confirm that the purpose of s. 7(3)(c.1) is to allow organizations to collaborate with law enforcement and national security agencies without a subpoena, warrant or court order. Organizations who share information with government institutions, including law enforcement and national security agencies, in accordance with the requirements of this provision, are doing so in compliance with PIPEDA.

Meanwhile, the Commissioner, in responding to the 2007 “lawful access” consultation, also clearly outlined the intent of section 7(3)(c.1):

Paragraph 7(3)(c.1), in contrast, is clearly intended to allow organizations to disclose personal information without consent or notification to LE/NS agencies and other government bodies in the absence of prior judicial authorization. However, the organization requesting the information has to identify its legal authority and indicate that it is collecting the information for one of the reasons listed in the paragraph, for example to enforce a law of Canada, a province or a foreign jurisdiction.

When the legislation (Bill C-6) was being debated in the House of Commons, the Minister of Industry clearly stated that 7(3)(c.1) was intended to maintain the *status quo*, “These amendments do not grant new powers to government institutions, nor do they create new obligations on business”. Although 7(3)(c.1) was not intended to alter the *status quo* we appreciate that it may have created some uncertainty on the part of organizations being asked to disclose certain information.

This provision was the subject of a considerable amount of discussion during the mandatory five year review of PIPEDA conducted by the House of Commons Standing Committee on Access to Information Privacy and Ethics. In its report,

¹⁴ Public Safety Canada, Customer Name and Address Information Consultation, September 2007.

tabled on May 2, 2007, the Committee recommended that consideration be given to clarifying what is meant by “lawful authority” in section 7(3)(c.1).

...The Privacy Commissioner has stated publicly that she would not object to adding definition for the terms “lawful authority” and “government institution” if the government feels that such definitions would bring clarity to the legislation.

Although the consultation paper identifies the “absence of explicit legislation” as one of the problems the consultation process seeks to address, *PIPEDA is, in fact, an explicit legislative code that permits lawful access by LE/NS agencies while “preserving and protecting the privacy and other rights and freedoms of all people in Canada”*. [Emphasis added]

C. Options for Further Clarification

If further clarification to section 7(3)(c.1) is required, we discuss three possible options: i) amend PIPEDA to introduce a new definition of “lawful authority”; ii) consider a regulation pursuant to section 26 of PIPEDA; or iii) have either Industry Canada or the Commissioner issue guidelines in collaboration with LEAs, industry and other stakeholders. As noted above, the greatest area of uncertainty has arisen in the context of requests from LEAs, as opposed to requests from a government department or agency with enabling legislation. Any additional steps to address remaining uncertainty should target that particular context.

(i) New definition of “lawful authority” in PIPEDA

Of the three options, we believe that this is most difficult from a drafting perspective. We suggest legislative amendment may be unnecessary, given the statements of clarification made to date and the other available options.

(ii) A regulation pursuant to section 26 of PIPEDA

There is a regulation-making power in PIPEDA to define “government institution”, and a more general regulation power for carrying out the purposes and provisions of PIPEDA. While a simpler process than legislative amendment, a new regulation would also face drafting challenges in attempting to clarify phrases like “lawful authority”.

(iii) Guidelines

The intent of PIPEDA may be inadvertently narrowed by option (i) or (ii). However, constraints of drafting for legislative or regulatory purposes do not exist for guidelines. Further, section 7(3)(c.1) of PIPEDA is a discretionary provision, rather than mandatory.

Given the structure of PIPEDA and the statements of clarification over the last few months, guidelines may be sufficient to provide any additional clarity required. This approach is taken in Service Alberta's guidance document, *Requesting Personal Information from the Private Sector: Forms and Guidelines for Law Enforcement Agencies*. In dealing with the requirement to identify a government institution's "lawful authority", the *Guidelines* state:

[S]ome statutes provide an agency with specific investigative powers that may include information-gathering powers, as in the case of investigations pursuant to the *Alberta Occupational Health and Safety Act*, or as identified in the duties and powers provided to police officers under section 38(1) of the *Police Act*.¹⁵

This approach would allow Industry Canada or the Commissioner to collaborate with stakeholders to better understand where uncertainty remains and to issue collaborative guidelines that meet the needs of both LEAs and the private sector, while preserving the privacy rights of individuals. The CBA Section welcomes the opportunity to collaborate on drafting guidelines.

V. INVESTIGATIONS AND INVESTIGATIVE BODIES

The CBA Section believes that a significant problem with PIPEDA is in the provisions regarding collection, use and disclosure of personal information in connection with an investigation.

In our 2005 submission, we made the following points about the current "investigative body" consent exemptions, saying that they:

- lead to confusion regarding the application of principles of agency law and the "third party processor" relationship that investigative bodies have with their clients;
- have unnecessary qualifications (e.g. requiring that a disclosing organization must disclose on its "own initiative");
- lead to inconsistent results because they lack a reciprocal consent exemptions (e.g. an organization has the right to collect, but the party from whom it has the right to collect does not have the right to disclose); and
- have inadvertently led to confusion about the application of PIPEDA. That has led to organizations which *prima facie* do not appear to be

¹⁵

Service Alberta's guidance document, *Requesting Personal Information from the Private Sector: Forms and Guidelines for Law Enforcement Agencies* at 10.

involved in commercial activities and so not governed by PIPEDA (e.g. the provincial CGA associations) voluntarily submitting applications to be investigative bodies and as part of that process, being required to demonstrate compliance with PIPEDA.¹⁶

The CBA Section recommended:

- eliminating the investigative body designation process;
- adopting the Alberta and BC PIPAs' approach, so the right to collect would include a reciprocal right to disclose;
- adopting the PIPAs' approach so collection, use and disclosure without consent would be permitted if for the purposes of an investigation (i.e. there is no requirement that a person meet the investigative body requirement for the exemption, and no need to apply to be designated as same); and
- adopting the PIPAs' more express approach to third party processing, so the definition of an organization would include any person working on behalf of that organization, such that in this context an investigator would be considered an agent of their client.

In addition to the anomalies inherent in the current investigation provisions of PIPEDA, the CBA Section believes that the application process to become an investigative body is so onerous, given the prohibitive cost of developing and submitting the application, that it is practically unavailable to all but the most well funded organizations. By adopting reciprocal disclosure rules and the provisions regarding investigations, distortions that have occurred as a result of a need to qualify as an investigation body would be alleviated.

We strongly agree with conclusion in the Government Response that further examination of the approaches taken by Alberta and BC is required, and that further consideration be given to how best to streamline PIPEDA's investigation provisions to make the process both more effective and logical, and to allow better harmonization with the provinces and territories.

VI. PARTS (PRIVACY AWARENESS RAISING TOOLS)

The Government Response asks for comments on Recommendation 17 of the Standing Committee Report, "the extent to which elements contained in the health-related PIPEDA Awareness Raising Tools (PARTs) document may be set out in legislative form". The

¹⁶ *Supra*, note 2 at 28-29.

application of PIPEDA to the health sector has created uncertainties, particularly as it was not designed to apply and recognize the particular sensitivities and complexities of health information. The PARTs questions and answers appear intended to dispel some of these uncertainties.

However, the CBA Section believes it is neither simple nor advisable to merely append the PARTs questions and answers to PIPEDA. This could increase rather than decrease ambiguity, given that they were not drafted in legislative or regulatory language.

Instead, the CBA Section recommends that after further review by the Commissioner, the PARTs questions and answers be adopted as formal guidelines issued by that office, which would create more certainty as to its status. Industry Canada's web site currently references the PARTs document, indicating that the Commissioner was involved in the drafting process, but the document is not an official guideline on the Commissioners' own website.

VII. IMPACT ON THE LITIGATION PROCESS

In our 2005 submission, the CBA Section argued that PIPEDA should be neutral in regard to the litigation process. We recognize that PIPEDA contains certain specific exceptions to the consent requirement to address the need for collection, use and disclosure of personal information in connection with the litigation process. However, in addition to the difficulties caused by the provisions regarding investigations and investigative bodies discussed earlier, there are many circumstances in the normal course of litigation that are not addressed by these exceptions.

A. Investigations and Witness Statements

Following the BC and Alberta legislative model, we have recommended excluding information available by law to a party in a proceeding. PIPEDA's treatment of investigations and witness statements collected as part of investigations illustrates the inadvertent impact of the legislation on established litigation procedures.

A party to a proceeding or anticipated proceeding may collect personal information without consent of the individual subject of the information under section 7(1)(b). If the person

providing the information is a private individual, that person is not prevented from disclosing it to the collecting organization. However, if an organization or an individual on behalf of an organization is providing the information, PIPEDA only permits disclosure with the consent of the data subject, by court order (section 7(3)(c)), or to an investigative body (section 7(3)(d)). In other words, the party may collect the information from an individual, but not from another organization because the other organization *may not disclose it* unless one or more of these requirements is met.

PIPEDA also permits individuals to access witness statements that contain their personal information. Access to witness statements may identify the witness, reveal documents subject to litigation privilege and circumvent longstanding rules of civil procedure and discovery.

A further anomaly is that an investigative body is not clearly characterized as the agent of the organization. If the agency relationship were clearly recognized in this context, it would resolve problems for an organization disclosing information without consent to an investigative body or to a second organization that has retained the investigative body as its agent.

The exceptions to the consent requirement in section 7 appear to have unintended consequences. Information may be collected and used by an organization without restriction, but may only be disclosed if specific conditions are met. One of the likely unintended consequences of this has been a proliferation of organizations seeking approval as “investigative bodies”, as discussed above.

An approach similar to that found in the Alberta and BC legislation would allow collection, use *and disclosure* of personal information where reasonable for the purposes of an investigation. This approach would remove a significant anomaly and some rigidity in PIPEDA in relation to the litigation process.

B. Other Effects on the Litigation Process

PIPEDA has also had an adverse or unnecessary impact in a number of non-court-ordered exchanges of information between parties, non-parties, and counsel. Sections 7(3)(a)-(c)

provide for disclosure to legal counsel, disclosure in connection with collecting a debt, and disclosure by court order, subpoena or in accordance with court rules regarding discovery. Many forms of legal disputes, ranging from personal injury, to professional discipline, to commercial disputes, involve collection, use or disclosure of personal information. The following examples illustrate some problems that occur:

- **Fact-gathering:** Although section 7(3)(a) permits clients to disclose personal information to their lawyer, there is no express exception for the lawyer to collect, use or disclose personal information and no exclusion for lawyers acting on behalf of their clients. In many instances, the lawyer is simply the agent of the party, yet PIPEDA appears to treat lawyers as separate collectors of information. For example, in Case Summary #340, two law firms were found to have breached PIPEDA. Acting for their clients to obtain credit reports about an individual for the purpose of potential litigation, the law firms were held to have engaged in commercial activities.¹⁷ However, in such circumstances, one could argue that the clients, if they were subject to PIPEDA, were entitled to collect the information under section 7(1)(b) and that the lawyers were simply acting as agents and therefore not prohibited from collecting the information.
- **Witness interviews, experts and investigators:** Clients can disclose personal information to their lawyer, but there is no provision in PIPEDA (except in collecting a debt) permitting disclosure to others potentially involved in the litigation process, such as witnesses, forensic accountants, private investigators, third parties, other lawyers, or expert witnesses. There is also no exception for such parties to further disclose the information, for example, in an expert report.
- **Pleadings:** PIPEDA affects lawyers' ability to effectively draft pleadings, many of which disclose the personal information of individuals without their knowledge or consent. Although PIPEDA permits the disclosure of personal information without knowledge or consent where required by law (section 7(3)(i)), it is unclear if this exception would extend to including personal information in pleadings.
- **Discovery:** There is no exemption in PIPEDA for oral disclosures made during discovery or court proceedings. The specific exception contained in section 7(3)(c) refers to "production of records". While a party may refuse material questions by arguing that an answer may involve information where disclosure is prohibited by PIPEDA, such a refusal can be overturned by a court order on motion. Recourse to the courts, however, results in not only increased legal costs between the parties, but further strains the legal system as a whole by a proliferation of otherwise

¹⁷

PIPEDA Case Summary #340, "Law firms collected credit reports without consent" (May 2, 2006).

unnecessary motions. The Alberta and BC PIPAs expressly resolved this issue by using the phrase “production of information”.¹⁸

- **Mediation, Arbitration and Settlements:** PIPEDA contains no exception for personal information collected, used or disclosed in the context of mediations, arbitrations and settlements. This hampers parties’ abilities to prepare for and engage in meaningful alternative dispute resolution. The exception to the access rule for information generated in the course of a formal dispute resolution process should extend to information generated in mediations and settlement processes.

These examples demonstrate that the narrow matrix of exceptions in section 7 of PIPEDA is inadequate in the unique context of legal proceedings. Generally, in litigation, the need is for full disclosure of relevant information so that the truth may be ascertained. Full disclosure facilitates proper adjudication and contributes to the settlement of disputes. Parties must be able to make out their claims and answer the claims of others. Balancing privacy in the context of the proper administration of justice requires different considerations than those at play when privacy is balanced against ordinary business needs. In the context of legal proceedings, we believe that courts are in the best position to balance privacy considerations against the need for full disclosure in litigation and note that they have filled this role for many years, without data protection laws.

Rules of court and the common law have incrementally evolved into a substantial body of law addressing privacy concerns independent of private sector data protection laws.¹⁹ For example, in *M.(A.) v. Ryan*, the Supreme Court of Canada addressed the need for full disclosure and the need for exceptions to that fundamental proposition:

...everyone owes a general duty to give evidence relevant to the matter before the court, so that the truth may be ascertained. [...] I accept that a litigant must accept such intrusions upon her privacy as are necessary to enable the judge or jury to get to the truth and render a just verdict. But I do not accept that by claiming such damages as the law allows, a litigant grants her opponent a licence to delve into private aspects of her life which need not be probed for the proper disposition of the litigation.²⁰

¹⁸ See e.g. Alberta *Personal Information Protection Act*, c. P-6.5, section 20(e).

¹⁹ The implied undertaking rule, for example, is fundamentally a privacy rule. See P. Matthews and H.M. Malek, *Discovery* (London: Sweet & Maxwell, 1992) (“The primary rationale for the imposition of the implied undertaking is the protection of privacy” at 253).

²⁰ [1997] 1 SCR 157, at paras. 19 and 38.

In our 2005 submission, the CBA Section recommended that PIPEDA be amended to reflect the approach of the BC and Alberta PIPAs to exclude information available by law to a party in a proceeding. The BC and Alberta PIPAs recognize that data protection laws are ill-suited in the context of legal proceedings. They include broad exceptions to consent for information collected, used and disclosed in relation to investigations and proceedings,²¹ expressly state that they do not limit the information available by law to a party to a proceeding,²² and provide that information collected for an investigation or legal proceeding is exempted from the access provisions of the laws. Alberta's law also contains an appropriately broad statement to the effect that it does not interfere with any legal privilege.²³ PIPEDA's exception is narrower and only protects solicitor-client privilege in the context of access requests.²⁴

When parties violate the proper bounds of litigation, for example, by collecting, using or disclosing personal information that is irrelevant to the proceeding, they can be subject to both sanctions under PIPEDA and possibly within the litigation itself. The collection, use and disclosure of personal information in the context of legal proceedings should be governed by longstanding rules designed expressly for that context.

The concerns that motivated the CBA Section's recommendation have also been reflected by some courts. In 2004, the Ontario Superior Court warned that PIPEDA could substantially disrupt Canada's civil and criminal litigation systems:

The legislation in question is complex and so broadly worded that a reasonable argument could be made to extend its reach so far as to transform both civil and criminal litigation into something very different than it is today.²⁵

The Standing Committee Report also recommended the approach of the PIPAs. However, the Response indicates that the Government does not agree that an amendment is necessary at this time.

²¹ BC PIPA, ss. 14(d), 17(d) and 20(m); Alberta PIPA ss. 12(1)(c), 15(1)(c) and 18(1)(c).

²² BC PIPA, s. 3(4); Alberta PIPA s. 4(5)(b).

²³ Alberta PIPA, s. 4(5)(a).

²⁴ PIPEDA, s. 9(3)(a).

²⁵ *Ferenczy v. MCI Medical Clinics*, 2004 CanLII 12555 (Ont SC) at paragraph 27; aff'd 2005 CanLII 18186 (Ont CA).

The CBA Section urges the Government to reconsider, given the potential ongoing distortion to the litigation process. We propose consideration of a broad-based exclusion for personal information collected, used or disclosed in the context of a proceeding, and specific amendments to address the deficiencies that we have identified in connection with investigations, information required in connection with proceedings and alternative dispute resolution processes.

We are also concerned that the law may be routinely honoured only in the breach, as parties and their counsel adhere to normal litigation practice, irrespective of any restrictions that PIPEDA may impose. This would not generate respect for the law, and is clearly an undesirable result.

VIII. CONCLUSION

The CBA Section trusts that our comments will assist in implementing the objectives outlined in the Government Response. We would be pleased to respond to any questions and to provide further information regarding any of the items addressed in this submission or otherwise in connection with that implementation.