

**Submission to the House of Commons Standing Committee on Access to
Information, Privacy and Ethics
Considering
The 2006 Review of the Personal Information Protection
and Electronic Documents Act (PIPEDA)**



Public Interest Advocacy Centre
ONE Nicholas St, Suite 1204
Ottawa, Ontario
K1N 7B7
Tel: 613-562-4002 ext.25
Fax: 613-562-0007

October 23, 2006

TABLE OF CONTENTS

OVERVIEW _____	3
EXECUTIVE SUMMARY _____	4
THE ISSUES _____	6
1. THE PRIVACY COMMISSIONER’S POWERS _____	7
a) Lack of Order-making power _____	7
b) Under-utilization of Current Enforcement Tools _____	10
c) Naming of Names _____	11
d) Findings Summaries _____	12
e) Fact Finding _____	13
Recommendations: _____	13
2. CONSENT _____	14
a) Consent Provisions are too Vague _____	14
b) “Blanket” Consent _____	17
Recommendations: _____	18
3. DUTY TO NOTIFY _____	18
Recommendations: _____	21
SUMMARY OF RECOMMENDATIONS _____	22

OVERVIEW

The Public Interest Advocacy Centre (PIAC) has historically been engaged with issues arising from the inappropriate collection, use and disclosure of personal information by organizations for commercial purposes, as well as ongoing law reform and review processes associated with Canada's current privacy legislation. For example, PIAC participated in the Senate Committee hearings on Privacy and Security on the Internet and the Senate Committee hearings concerning the Do-Not-Call Registry (Bill C-37). PIAC already has studied PIPEDA's effectiveness from a consumer perspective and made recommendations in a report, "Consumer Privacy under PIPEDA: How Are We Doing?" PIAC, (November 2004), to relevant policymakers. PIAC also has recently completed studies of privacy-related issues such as the use of radio frequency identification (RFID) by major retailers, and biometrics and national ID cards.

PIAC's goal is to help Parliament ensure that PIPEDA is the most effective vehicle for fulfilling Parliament's stated objective in PIPEDA – recognizing the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information "for purposes that a reasonable person would consider appropriate in the circumstances."

This brief contains the consumer position advanced by PIAC concerning the five-year legislative review of the Personal Information Protection and Electronic Documents Act (PIPEDA) undertaken by the House of Commons Standing Committee on Access to Information, Privacy and Ethics. In this brief, PIAC has sought to provide the Committee with comments on the five-year track record of the Act to date, as well as recommendations for reforms to improve the overall effectiveness and clarity of the Act. The purpose of this brief is to present consumer views in a manner that will be helpful to the Committee during its review of PIPEDA.

EXECUTIVE SUMMARY

Issues

The 2001 enactment of PIPEDA adopted, with a few modifications, the Canadian Standards Association's *Model Code for the Protection of Personal Information*. Although the Model Code has the advantage of flexibility, its language is ambiguous and vague on key concepts. These structural shortcomings have led to certain unanticipated and unwanted negative effects on consumer privacy. PIAC has identified three areas of particular concern, namely: (1) the privacy Commissioner's enforcement powers; (2) the "consent" provisions; and (3) inclusion of a "duty to notify" in cases of data breaches.

1. The Privacy Commissioner's Enforcement Powers

PIPEDA lacks an effective enforcement mechanism; in particular, the Commissioner does not have the power to make binding orders. Enforcement is only available through the Federal Court, which is costly to the complainant in both time and money. The lack of this power permits ongoing non-compliance by organizations. An "ombudsman with a stick" model – where the privacy commissioner has binding order powers, as in British Columbia, Quebec and Alberta – would offer a number of advantages over the current model. PIAC strongly recommends that the powers of the Commissioner be amended to provide for an order-making power.

A further problem is the under-utilization of current enforcement tools, specifically: the continued reticence of the Office of the Privacy Commissioner of Canada (OPCC) to engage in privacy audits of businesses and industries; its tendency to respond to external complaints rather than initiating its own; and the lack of follow up on OPCC recommendations.

The lack of enforcement powers is exacerbated by the policy of the OPCC generally not to name an offending organization, even in the face of "repeat offenders", which generates little incentive for a large business to change an entrenched business practice. PIAC recommends the OPCC adopt the policy of 'naming names'.

The OPCC policy of issuing only select summaries of the Commissioner's findings on complaint investigations impedes the ability of lawyers, businesses and privacy consultants to understand the law or their privacy responsibilities. Full, published decisions are a crucial resource for organizations in evaluating the law and determining how they can meet its requirements.

In addition, procedural rules governing the investigation process where facts are disputed should require the exchange of submissions prior to and during the investigation, with the ability to arrive at an "agreed statement of facts" before the OPCC concludes the investigation.

2. The “Consent” Provisions

Defining consent is one of the biggest challenges in reforming PIPEDA. PIAC has identified two areas in which the current consent requirements under PIPEDA are lacking: vagueness and blanket consent. The language of the consent provisions is ambiguous. At present, “implied consent” might be enough with less “sensitive” information, but express consent will be necessary where the information is likely to be considered more “sensitive”. PIAC believes PIPEDA should be amended to clearly state that the standard of consent to be applied throughout the Act is that of “informed consent”. PIAC recommends that the definition of consent in PIPEDA be re-written to require that consent be manifest, free, enlightened, given for a specified purpose and that consent be a continuous process.

Organizations have created privacy policies and consent clauses that are so broad as to capture consent for any and all collection, use and/or disclosure that the organization could conceivably desire in the future. Blanket consent takes advantage of the unequal bargaining power that often exists between consumers and organizations. PIAC recommends that PIPEDA be amended to specifically prohibit the use of blanket consent statements.

3. Inclusion of a “Duty to Notify”

With the rise of identity theft in Canada, business that handle and deal in personal information must be held accountable for their security practices and there must be enforcement mechanisms in place to ensure that organizations comply with the reporting requirements. PIAC recommends that PIPEDA be amended to include a similar notification requirement to that of California’s *Security Breach Information Act*, and to impose a legal “duty to notify” consumers of any loss or theft of personal information.

THE ISSUES

In 2001, Parliament introduced PIPEDA to protect the personal information of Canadians consumers from inappropriate collection, use and disclosure by organizations in the course of commercial activities. At the time PIPEDA came into effect, it was heralded as an innovative, flexible and responsive legislative answer to the privacy concerns of Canadians. However, as with most new legislation, gaps began to appear once its provisions were put into practice. Armed with the insight and experiences of the past five years, we are now at an optimal stage to re-examine Canada's private sector privacy legislation.

Before examining specific areas for reform, it is important to understand the underlying causes of the disunity between the Act and its practical application. The most important single cause of consternation for businesses, practitioners and consumers is the lack of clarity and certainty afforded under the Act.

During the drafting process, Parliament took the unusual step of forgoing a complex drafting exercise in favour of adopting, with only a few legislative modifications, an industry code based on the Canadian Standards Association's *Model Code for the Protection of Personal Information*. Essentially, PIPEDA enacts into law the "ten privacy principles" and commentaries contained in the CSA's Model Code. Incorporating what is essentially an industry standard so explicitly into federal legislation is something of an innovation for a Canadian federal Act. Unfortunately, this innovative feature has created numerous challenges for businesses and practitioners who seek clarity and certainty in the law.

The CSA's Model Code is one of the best examples of its kind - no doubt why the federal government was so eager to adopt it. However, it was drafted to achieve practical consensus among industry participants, not to become law of the land. As such, its language is necessarily vague and ambiguous. As privacy law practitioners point out, "[f]rom the lawyer's technical perspective, to attach an unamended private industry code of conduct to a statute, giving it force of law, is to codify vague and ambiguous language that leaves plenty of room for argument."¹

On the other hand, the unique features of a Model Code present numerous advantages for policy-makers. The flexibility inherent in a set of broadly-worded standards allows for greater manoeuvrability on the part of the Privacy Commissioner to respond to various privacy issues, and provides the Commissioner with a wider array of legislative options at her disposal. For instance, the ten privacy principles have been applied to extend the reach of PIPEDA. The "Openness" principle, for example, has been used by the Privacy Commissioner as grounds for mandating that organizations choosing to employ service providers located in the U.S., notify customers that their personal information is processed outside of Canada and may be subject to disclosure to government authorities under applicable U.S. law, such as the *USA Patriot Act*.²

PIAC feels that although the flexibility and manoeuvrability provided by the Model Code assist the Privacy Commissioner and her Office in responding quickly to, for example, technological change and the potential threat new technologies pose to consumer privacy such as RFID chips, this nimbleness comes at the expense of the certainty and effectiveness of the Act.

Rather than relying solely on vaguely worded standards, certain provisions are key, and must be drafted with practical commercial implementation in mind.

Keeping in mind the need to clarify the law and provide increased measures of certainty for all stakeholders, PIAC has identified three specific areas where reforms are needed:

- 1) The Privacy Commissioner's Powers;
- 2) The "Consent" Provisions; and
- 3) Inclusion of a "Duty to Notify" individuals when there is a "data breach" by the holder of their personal information.

Each of these issues will be discussed below, and reforms suggested, with a view to improving PIPEDA by increasing organizational compliance and consumer confidence in the law.

1. THE PRIVACY COMMISSIONER'S POWERS

The existing ombudsman model is ineffective at protecting the privacy rights of individuals and addressing the legitimate interest in personal information of organizations engaged in commercial activities.

There are several important reasons why the existing ombudsman model is ineffective at protecting the privacy rights of Canadians. Each reason will be discussed along with recommendations on how best to remodel the role and functions of the Office of the Privacy Commissioner (OPCC) to better address the privacy needs and expectations of Canadians.

a) Lack of Order-making power

Simply stated, PIPEDA lacks an effective enforcement mechanism. The enforcement tools of an ombudsman-type commissioner are extremely limited and are largely inadequate to promote Canada's privacy agenda and meet the privacy expectations of Canadians.

The Act vests limited enforcement powers in the Privacy Commissioner of Canada. The Commissioner is authorized under the Act to receive complaints, conduct investigations and issues reports on her findings.³ The Commissioner is also obliged to develop and conduct information programs to encourage public understanding of the Act, to carry out and publish research on matters relating to the protection of personal information and to encourage the voluntary adoption by organizations of appropriate compliance practices and procedures.⁴

The importance of the role of the Privacy Commissioner, and the crucial functions of that Office, simply do not correspond with the limited nature of its powers. The Commissioner has been armed with the power to audit the privacy practices of organizations suspected of violating PIPEDA (although this power has rarely been used), and can receive, initiate and investigate complaints of non-compliance with the Act.⁵ However, a crucial, but missing, component in the Commissioner's enforcement arsenal is the ability to make binding orders. As such, the OPCC is

severely limited in the assistance it can provide Canadians who seek relief from a privacy-invasive practice. Instead, complainants (and the Commissioner on behalf of a complainant) are forced to refer non-compliance to the Federal Court of Canada. It is only here that remedial authority is available, including the power to award damages.

This lack of power to issue binding orders, assess penalties or impose sanctions permits (and breeds) on-going non-compliance by organizations. Upon finding a violation of the Act, the Commissioner has no enforcement power to compel an organization to make specific changes to their policies or practices; nor does it have the authority to reprimand an organization by way of fines or penalties. Absent the element of compulsion, an organization's decision regarding whether or not to comply with a finding by the Commissioner will typically be made on a business maximizing basis – i.e., the cost of compliance vs. the cost of non-compliance. For example, an organization may take into account the potential loss of customers, loss of productivity, loss of secondary marketing revenue, and the risk of legal costs from an application to Federal Court (usually a low risk given the high resources and costs to the complainant). Thus, the practical reality is that when faced with an entrenched, privacy-invasive, business practice that is perceived by the organization as an important process, it is not automatic that a negative finding by the Commissioner will alter the practice. Many organizations will make the strategic decision to ignore the Commissioner's findings and take the gamble that they will not face a negative decision in Federal Court.

In the *Eastmond*⁶ case, Canadian Pacific chose not to comply with the Commissioner's recommendations, obliging Mr. Eastmond to make an application to Federal Court in order to have the recommendations enforced. Similarly, in the *L'Écuyer*⁷ case, Ms. L'Écuyer made an application to Federal Court only after the airport failed (or elected not) to comply with the findings of the Commissioner. Although the Federal Court in both cases eventually overturned the Commissioner's decision, it is instructive that both parties felt compelled to apply to the Federal Court to enforce the Commissioner's finding, as the respondents presumably had indicated they would not implement the Commissioner's suggestions.

Unlike the Privacy Commissioner, the Federal Court, hearing an application made pursuant to the Act has a wide range of remedies available to it, including: the issuance of orders requiring an organization to correct its practices or to publish a notice of any action taken or proposed to be taken to correct its practices; an unlimited award of damages (including for "humiliation"); and an award of punitive damages. This is in addition to any other remedy within the jurisdiction of the Federal Court to grant.⁸

As the process in section 14 does not provide for an appeal of the Privacy Commissioner's findings, the Federal Court hears such applications "*de novo*." Nevertheless, the Federal Court has recognized the specialized expertise of the Commissioner, and has been willing to grant her at least notional deference. In *Englander v. Telus Communications Inc.*,⁹ Blais, J. held that the Privacy Commissioner, "...as a statutorily created administrator with specialized expertise... is entitled to some deference with respect to decisions clearly within his jurisdiction."¹⁰

While the Federal Court *may* afford some deference to the Commissioner's findings, there is no obligation to do so. This lack of legal weight leaves the Commissioner's findings of questionable

legal significance, and arguably of little guidance to other organizations with similar business practices (and of no guidance at all when findings are not published under the OPCC's optional publication policy). Moreover, the status of the Commissioner's legal findings was made very clear in *Englander*,¹¹ when Justice Décaré stated that:

The Commissioner... is not a tribunal and has no decision-making power under the PIPED Act. At best, the Commissioner can form an opinion on the issue and include it in his report. As the report is not a "decision," there can be no conflict with the decision of a court or tribunal found to have exclusive, concurrent or overlapping jurisdiction to determine the issue.¹²

Further reducing the weight of Privacy Commissioner decisions is the fact that Federal Court hearings reconsider the facts (even those of the initial privacy investigation), thereby allowing or requiring the parties to a Federal Court enforcement action under s. 14 of PIPEDA to re-prove evidence.¹³

Enforcement today is thus only available upon a successful application by a complainant to the Federal Court. Such applications have been rare in the short history of the Act. Moreover, applications under s. 14 are likely to remain low given the high costs and enormous effort required by a complainant to pursue such an application (not to mention the risk of an award of costs).¹⁴ Thus, for a consumer to get what they typically seek in a complaint – full compliance with PIPEDA by the target organization – there is in fact only one very long and expensive way to ensure this.

In stark contrast to this arguably ineffective ombudsman model, lies the successful use of order-making power on the part of numerous provincial Commissioners. Among the most prominent differences between PIPEDA and its provincial counterparts relates to the degree of remedial authority granted to the provincial privacy Commissioners. Unlike her provincial counterparts, the federal Commissioner lacks the power to issue final decisions settling disputes and issue enforcement orders (subject to judicial review). In all three provinces with “substantially similar” legislation to PIPEDA, each has chosen a more powerful model and has granted their respective privacy Commissioner's order-making powers. Québec, Alberta and British Columbia have each opted for the model that has been referred to as an “ombudsman with a stick”.¹⁵

Support for this “ombudsman with a stick” model is continuing to grow. The Offices of the Information and Privacy Commissioners (OIPC) recently acknowledged that:

Commissioners in most of these provinces use this power sparingly, preferring whenever possible to resolve complaints through conciliation, mediation, and other informal means. They nonetheless consider the existence of this power, which provides a strong incentive to the parties to settle on reasonable terms, to be essential to their effectiveness.¹⁶

Moreover, the OIPC concluded that: “In most of the provinces that have adopted this model, the process has not become overly formalized, and the commissioners have been able to attain very high settlement rates.”¹⁷

Similarly, the Access to Information Review Task Force,¹⁸ after conducting an extensive review of the *Access to Information Act*,¹⁹ concluded that a Commissioner with order-making powers represents “the model most conducive to achieving consistent compliance and a robust culture of access.”²⁰ The Task Force then went on to summarize the advantages of the order-making power as follows:

Many users would argue that a Commissioner with order-making powers would provide a more effective avenue of redress for complainants. Under the current system, a complainant who is not satisfied with a recommendation by the Commissioner or the government’s response must apply for review by the Federal Court. This is both time-consuming and expensive.²¹

While the conclusions of the Task Force were derived from an “access” standpoint, there is no reason why similar conclusions cannot be drawn from a “privacy” standpoint. Indeed, both the Information Commissioner and the Privacy Commissioner have very similar roles and responsibilities, which pit consumer and individual interests against corporate and organizational ones, and operate under much the same structures. Both are independent ombudsmen appointed by Parliament with investigative and mediation powers.

There is a clear trend towards the “ombudsman with a stick” model in Canada and for good reason: an order-making model provides a firm, immediate determination of the complaint, a more consistent body of jurisprudence, and a level of transparency and accountability that is sorely lacking in the current model.

b) Under-utilization of Current Enforcement Tools

The Office of the Privacy Commissioner of Canada also under-utilizes existing enforcement tools. Since the coming into force of PIPEDA five years ago, the OPCC has shown a continued reticence to engage in privacy audits of businesses and industries for systemic privacy violations. Section 18 of the Act permits the Commissioner, on reasonable notice and at any reasonable time, to conduct an audit of an organization’s information handling practices if the Commissioner has reasonable grounds for believing that the organization is contravening the Act. In carrying out an audit, the Commissioner possesses the same expansive powers as she does when conducting an investigation (i.e. the power to issue and enforce summons, compel testimony and documentary disclosure, administer oaths, and enter premises occupied by an organization).²² The Commissioner also enjoys a general right to delegate her audit powers.²³ Despite this significant array of audit powers, to date, the OPCC has failed to conduct a single corporate audit. Tellingly, the only audit that has been performed, of the Canadian Border Services Agency (CBSA), turned up serious irregularities and privacy violations.²⁴

Another important, yet underutilized tool is the ability of the Commissioner to initiate a complaint where no external complaint has come forward, if satisfied that reasonable grounds exist for conducting an investigation.²⁵ However, rather than take a proactive approach to

ensuring the privacy rights of Canadians, the OPCC has been largely content to wait and define PIPEDA solely through individual complaints.²⁶

Moreover, when the OPCC has issued recommendations to companies on a change of business practice to either: a) come into compliance with PIPEDA (sometimes within a specified timeframe), or b) as a suggested “best practice”, there appears to have been no follow-up of these recommendations by the OPCC. This lack of follow-up has occurred despite that fact that several companies have been found to be “repeat offenders”, facing well-founded complaints on the very same issue in succession. At the very least, companies should be advised that failure to follow recommendations will bring about an OPCC-led investigation or audit.²⁷

c) Naming of Names

The lack of enforcement powers is exacerbated by the policy of the OPCC generally not to name an offending organization (except in exceptional circumstances). While the Commissioner is generally required to maintain in confidence any information that comes to her attention as a result of the performance of her duties, she can reveal to the public details of the information management practices of an organization if she considers it to be in the public interest to do so.²⁸ Although the naming of the offending organization seems an obvious option, the OPCC has consistently refused to name respondents, even in the face of repeat offenders who continue to disregard the Commissioner’s recommendations. As a result, there is little or no incentive for a large business to change an entrenched business practice unless the Commissioner either has enforcement powers, or at the very least chooses to publish names, so as to enable the public to hold the perpetrators accountable.²⁹

The policy rationale for maintaining the anonymity of the complainant is clear. Confidentiality encourages individuals to bring claims forward, and given that a complainant is seeking relief from an invasion of privacy, naming them would simply throw salt on the wound. Similarly, PIAC feels strongly that complainant confidentiality ought to be carried through to applications before the Federal Court. Complainants who do not wish to be named ought to be referred to by initials or a pseudonym (similar to procedures for young offenders and victims of sexual assaults). Additionally, it is easy to anonymize the facts of a case so as not to inadvertently disclose the identity of the complainant. Forcing a complainant to reveal their identity in Federal Court in light of a privacy dispute is unnecessary and provides a strong disincentive for them to pursue their application. We certainly do not want to re-victimize the victim. However, the same rationale does not hold true for offending organizations.

In a 2003 speech, David Loukidelis, Information and Privacy Commissioner of British Columbia, commented on his province’s policy with regard to the naming of names:

Nor do I accept that organizations affected by formal decisions have a legitimate interest in remaining anonymous. In fact, the prospect of publication of the name of an organization that has breached the law is a necessary and legitimate sanction for non-compliance and incentive for compliance. Where a decision vindicates an organization, publication rewards compliance... An essential component of the rule

of law is that justice must be seen to be done and this holds true under a private sector privacy law no less than in litigation in the courts.³⁰

For a free market to work, a consumer needs to have as much information about a product or service supplier in order to make an informed decision about where to allocate their resources. The maximization of information available to consumers is in the public interest, as it allows for the maintenance of free and open markets for commercial activities. Knowing that an organization is not complying with PIPEDA in respect of their personal information could well lead a consumer to switch to a supplier that more fully respects their privacy rights. Consumers ought to have the ability to base their purchasing decisions on whether or not a company will treat their personal information with their desired level of privacy protection. Publicly naming an offending organization is the first step to providing transparency, accountability and choice to consumers.

The time has come to name names. Organizations have had several years to feel their way through Canada's privacy legislation and they must now be held publicly accountable for their actions. This is not to say that only privacy violators should be named, we would also support the public recognition of those organizations who have been outstanding in their commitment to ensuring privacy. Canadians ought to be given all information, good and bad, in order to make an informed decision about where, when and with whom to entrust their personal information. An amendment of PIPEDA that makes this policy clear is a necessary step.

d) Findings Summaries

Adding to the lack of transparency and accountability is the policy of the OPCC to issue only select summaries of findings of complaint investigations.

The Commissioner is required under PIPEDA to prepare and circulate *to the parties* a detailed report containing her findings and recommendations, within one year following receipt of a complaint.³¹ However, the public findings published on the OPCC website are merely summaries of the Commissioner's full findings and do not provide a complete understanding of the Commissioner's decisions or reasoning. The complainant and the respondent are instead the only parties provided a full letter of finding – but this letter may exist in different versions. Lawyers and privacy consultants have complained that the lack of detail and overall vagueness of the summary findings limit their ability to advise their clients or confidently state the law of privacy responsibilities.³² The findings reports are often so terse as to be unusable. In addition, the summary in at least one case appears to leave out important information in the full report that effectively changes the OPCC interpretation of the law.³³

David Loukidelis, B.C.'s Information and Privacy Commissioner, has expressed the need for the full publication of decisions in privacy-related disputes: "Formal decisions in specific disputes will be critical to development of the law and provide guidance to those affected by the law. It is therefore essential that these decisions be published, not in summary form, but in full."³⁴

Full, published decisions are a crucial resource for organizations in evaluating the law and determining how they can meet its requirements. Furthermore, individuals and organizations are entitled to certainty and predictability in the law that can only come with transparent and open decisions. We would therefore urge an amendment of PIPEDA that requires the OPCC, in line with a more formal investigation process and order-making, to publicly file one set of authoritative reasons with sufficient detail for the public to examine the decision's rationale.³⁵

e) Fact Finding

While the Privacy Commissioner has extensive powers of investigation, there are no apparent procedural rules in place to guide the investigation process where those facts are disputed by the parties. For example, there is no requirement for disclosure, and there are no rules allowing parties to test the facts as presented by the other side (no rules of evidence). For instance, in a complaint brought by PIAC in 2002, the respondent submitted additional facts to the OPCC that PIAC did not have the opportunity to see, let alone to test, before the Commissioner issued a ruling. The Commissioner's "revised letter finding" was based, at least in part, on these untested facts. At minimum, the process should require the exchange of submissions prior to and during the investigation, with the ability to arrive at an "agreed statement of facts" *before* the OPCC concludes the investigation.³⁶ Presumably with any order-making power would come a modicum of evidentiary process.

Recommendations:

The existing ombudsman model has largely proven ineffective at protecting the privacy rights of individuals. PIAC strongly recommends that the powers of the Commissioner be amended to provide for an order-making power, along the lines of those in Québec, British Columbia and Alberta data protection legislation. The powers of the federal Commissioner ought to be in line with those of her provincial counterparts and ought to reflect the growing trend towards enabling Commissioners to issue binding orders.

As a means to provide increase transparency and accountability in privacy-related matters before the Commission, PIAC recommends that the OPCC adopt the policy of publicly naming organizations which have been found by the Privacy Commissioner to have violated PIPEDA. As a necessary component, PIAC further recommends that the OPCC adopt the policy of issuing full, published decisions of complaint investigations.

It is however, imperative that complainants remain anonymous, both at the Commission level and at the Federal Court level. To force complainants to be publicly revealed in light of a sensitive privacy dispute would only serve to detract complainants from pursuing relief from legitimate grievances.

Finally, the OPCC needs to put in place specific procedural rules for the collection and disclosure of evidence before the Commission. Additionally, an "agreed statement of facts" ought to be sought in each case before the Commissioner issues a final ruling, if the

Commissioner does not otherwise obtain the power to make binding orders (which should imply a duty to make concrete factual findings with procedural safeguards for the parties to present and contest evidence).

2. CONSENT

PIPEDA is a consent-based statute. Generally it requires the knowledge and consent of the individual affected in order for the collection, use and disclosure of the individual's personal information for commercial transactions. As the Privacy Commissioner recently noted, "[r]econciling the consent principle with the realities and demands of the commercial environment presents several challenges."³⁷ One of the biggest challenges is in defining consent (and its exceptions) in a way that reflects commercial realities while at the same time providing adequate protections for consumers.

PIAC has identified two areas in which the current consent requirements under PIPEDA are lacking. They include:

- a) the overall vagueness of PIPEDA's consent provisions; and
- b) the need to specifically address the issue of "blanket consent";

Each issue will be discussed, and recommendations provided, on how best to address the legislative gaps, increase compliance, and better address the privacy needs and expectations of Canadians.

a) Consent Provisions are too Vague

PIPEDA's consent requirements are characterized by ambiguous language and amorphous standards. As a result, 'consent' has been subject to wide-ranging interpretation, while compliance with PIPEDA's consent provisions has suffered. Clarification of the consent requirements will help ensure that PIPEDA is interpreted and applied in a manner that achieves the objectives of the Act.

Schedule 1 of PIPEDA contains a broadly-worded "Consent Principle". This principle provides a general framework for thinking about consent for privacy purposes in a commercial context; however, its language provides very little in the way of concrete assistance to businesses and consumers looking for a definitive statement of what consent is, what consent is required under the Act and how to obtain it.

For instance, the Model Code instructs that when it comes to obtaining consent, "the form of consent sought by an organization may vary, depending upon the circumstances and the type of information."³⁸ Similarly, the Code instructs that "in obtaining consent the reasonable expectations of the individual are also relevant"³⁹ and that "the way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected"⁴⁰ It is obvious that these consent provisions permit both the organization and the individual to

argue that any processes set-up to obtain consent are deficient, or sufficient, from the point of view of either the individual or the business.

Regarding the form of consent that is required to comply with the Act, we find similar confusion. Implied consent *might* be enough with less sensitive information, but express consent will be necessary when the information “is likely to be considered sensitive”.⁴¹ Other information, which in certain settings would be innocuous, will, in other settings, be deemed highly sensitive. The consent principle in the Schedule goes on to unhelpfully provide that “any information can be sensitive, depending on the context”.⁴² In a nutshell, the Act does not explicitly adopt any one method of obtaining consent, leaving individuals and organizations the argument of whether the information is sensitive or not, rather than stipulating that certain methods of obtaining consent should be used to obtain certain types of personal information. For example, at present, and despite a number of OPCC rulings on the issue, businesses continue to use “opt-out” forms of consent which place the onus on the individual to restrict the scope of their consent – effectively deeming consent on the part of the individual by contract.

These difficulties with the form and adequacy of consent reveal the larger problem at issue with PIPEDA. It simply does not make any attempt to define this key concept of “consent”. Absent some definition in the Act, the definition has inevitably been left to the courts, which have returned the unambiguous answer that consent is the informed consent of the individual.

It is PIAC’s view that the case of *Englander v. TELUS Inc.*,⁴³ has thus conclusively established that ‘informed consent’ is the standard of consent in PIPEDA. The Federal Court of Appeal’s decision in *Englander* is the highest court interpretation of PIPEDA’s consent requirements to date, and as such, sets the bar very high for how future issues of consent must be measured. In *Englander*, the Court made it clear that the appropriate standard under PIPEDA is informed consent, stating:

“Principles 2, “Identifying Purposes,” and 3, “Consent,” are at the heart of this appeal. Principle 3, I hasten to add, despite its name, “requires ‘knowledge and consent’ ” (clause 4.3.2). ***In other words, Principle 3 requires informed consent.*** [Emphasis added.]”⁴⁴

A true “informed consent” standard sweeps away most of the uncertainties surrounding obtaining consent and the form of obtaining it. Generally, such a standard would mean businesses would be required to obtain explicit consent or a record of transactions that would demonstrate unambiguously that a reasonable person in the situation of the individual at the time of the transaction would have understood the extent of the consent to the use of his or her personal information and assented on that complete information. If a business did not reveal all of the intended uses or disclosures of the personal information to the individual, the business would face an uphill battle in attempting to demonstrate this full and informed consent. Practically speaking, this would mean that businesses would have to wean themselves from reliance on opt-out consent mechanisms, avoid making the consumer work to find the relevant privacy policy or clause, and fully and accurately explaining in layman’s language the intended sharing of the information.

A recent study by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) highlighted this failing.⁴⁵ The CIPPIC study was designed to assess the compliance level of retailers with certain key provisions of PIPEDA. The study assessed the compliance of 64 online retailers with PIPEDA requirements for Openness, Accountability and Consent. It also assessed the compliance of 72 online and offline retailers with the PIPEDA requirement for Individual Access. In evaluating the results of their study, CIPPIC concluded that the results “indicate widespread non-compliance with all four areas.”⁴⁶ In the area of consent especially, the study found numerous opt-outs, incomplete or non-existent descriptions of personal information handling and onerous steps for the individual to understand the companies’ uses and disclosure of their personal information. All of these practices violate PIPEDA’s consent standard.

The most effective way to address this “widespread non-compliance” is to directly address the ambiguities in the consent provision. Organizations should be given a clear and concise phrasing outlining the legislative requirements for obtaining consent and in what circumstances the different types of consent are appropriate.

To assist businesses in approaching this standard, PIPEDA should be amended to clearly state that the standard of consent to be applied throughout the Act is that of “informed consent” (i.e. the requirement of knowledge and consent), except where clear exceptions to this requirement are provided for. The clear requirement to explain, at or before the time of collection, *all* the uses to which person information will be put, is the essence of informed consent and should be the baseline requirement of the Act.

PIAC is aware that in certain commercial situations, a lower standard of consent may be appropriate, however, we stress that such situations should be strictly limited. In order to avail themselves of such exceptions (for example, in certain situations, Parliament may judge that a simple notice of personal information use or an opt-out mechanism would be appropriate), which should be rare, the organization also should face the burden of demonstrating there is a) a clear commercial need for the information for that particular transaction; b) no alternate method for obtaining an informed consent short of undue hardship and c) if a lesser consent standard is selected, that it is the least intrusive possible method and that the individual is informed to the greatest extent possible in the circumstances.

PIAC therefore recommends strengthening the consent requirements under PIPEDA by including the following principles in a consent definition, which are consistent with informed consent:

- Consent must be manifest - meaning that it is clear, certain and indisputable;
- Consent must be free - meaning that it must be given without compulsion;
- Consent must be enlightened - meaning that it must be precise, rigorous and specific;
- Consent is also given for a specified purpose; and
- Consent is a continuous process – meaning it is to be given for the length of time needed to achieve the purposes for which it was requested. The length of time will not necessarily be related to a number of days, months or years, but may refer to a specific event or situation.⁴⁷

b) “Blanket” Consent

True consent involves more than a one-time, wide-open, blanket statement on a consent form. Rather, informed consent is a dynamic process that involves transparency, full disclosure, and active engagement by both parties.

The worst solution to documenting informed consent is the form that blankets all possibilities. This type of consent, known as “blanket consent”, is essentially worthless. Consent is only meaningful if the individual understands how it will be used. Nevertheless, these all-encompassing blanket statements have started to appear with alarming frequency in the course of consumer transactions.⁴⁸ In large part, blanket consent is a business practice that has developed as a means of getting around the vaguely-worded consent provisions in PIPEDA. Organizations have created privacy policies and consent clauses that are so over-broad and all-inclusive, that they seek to capture consent for any and every possible collection, use and/or disclosure that the organization could conceivably desire in the future.

These “blanket consent” statements seek to take advantage of the unequal bargaining power that often exist between consumers and organizations. Where individuals are in relationships of unequal bargaining power, there may be pressure to provide, what in essence amounts to a blanket consent, where a customer may otherwise be reticent to do so. Furthermore, consumers may be providing a blanket consent without even knowing it. For example, in a recent survey of bank customers conducted for Advocis, it was found that 42 percent of respondents who were contacted by banks with information about more products and services believed that they had not consented to having their personal financial information reviewed by the bank.⁴⁹ According to Advocis, “[m]any of these respondents might have signed broadly worded consent forms and not fully appreciated the scope of the consent given.”⁵⁰

PIAC suspects that much of the “blanket” consent language in many privacy policies is actually designed to avoid PIPEDA principle 4.2.4, which requires notification *and consent* of the individual when information that was gathered for one purpose is proposed to be used for another purpose. It may also signal an attempt by an organization to avoid the effect of principle 4.3.3, the “refusal to deal” section, which essentially stipulates that a business may not make a sale conditional on collection of more personal information that is necessary for the particular transaction.

It seems obvious that consent clauses should be easy to find, clear and straightforward in their language, and not blanket statements. However, as the CIPPIC survey clearly demonstrates, a large number of organizations are not respecting the requirement for informed consent.⁵¹

Although such clauses clearly could be challenged by consumers as overbroad and not respecting the consent requirements of PIPEDA, in order to remove the burden on consumers of complaining about each violation, PIAC recommends that PIPEDA be amended to specifically prohibit the use of blanket consent statements as a means of obtaining consent. Therefore, “blanket consent” statements could be deemed void under a definition in the Act. Such a definition would rely in large part upon a prohibition on seeking consent to future events, which also is consistent with Principles 4.2.4 and 4.3.3., as noted above.

Recommendations:

PIAC recommends that PIPEDA be amended to clearly state that an “informed consent” standard is the appropriate measure to be applied throughout the Act, except where clear exceptions to this requirement are provided for. Such an amendment would serve to reduce uncertainties in the Act and provide organizations with a clear standard for which to judge compliance. Furthermore, such an amendment would reflect the Federal Court of Appeal judgment⁵² that “informed consent” is the appropriate standard of consent in PIPEDA.

PIAC further recommends strengthening the consent requirements under PIPEDA by including the following principles:

- A clear definition of consent in the Act that makes clear the standard is one of ‘informed consent’, meaning:
 - Consent must be manifest - meaning that it is clear, certain and indisputable;
 - Consent must be free - meaning that it must be given without compulsion;
 - Consent must be enlightened - meaning that it must be precise, rigorous and specific;
 - Consent is also given for a specified purpose; and
 - Consent is a continuous process – meaning it is to be given for the length of time needed to achieve the purposes for which it was requested. The length of time will not necessarily be related to a number of days, months or years, but may refer to a specific event or situation

In addition, PIAC recommends that PIPEDA be amended to specifically prohibit the use of “blanket consent” statements as a means of obtaining consent. Although it seems clear that such statements are prohibited under the current wording of PIPEDA, it is equally clear that organizations continue to disregard the informed consent standard. Therefore, it is PIAC’s view that the inclusion of an unequivocal prohibition on the use of “blanket consent” statements is needed to increase compliance and address issues of ambiguity in the Act.

3. DUTY TO NOTIFY

Organizations that suffer loss or theft of personal information should have a legal duty to report the loss or theft. Furthermore, there should be enforcement mechanisms in place to ensure that organizations comply with the reporting requirements.

The loss or theft of personal information has become a serious threat to an individual’s personal and financial security. The increasing accumulation of personal data by organizations and the widespread consolidation of databases, have left individuals vulnerable to abuses by those with access to the data (whether lawful or unlawful).⁵³ Identity theft has become one of the fast growing crimes throughout the world – it is also proving persistently difficult to combat. The perpetrator can be anywhere in the world and can have no connection to the victim, aside from the pieces of personal information that have been stolen. Stealing an identity can enable an individual to commit all sorts of additional crimes under a pseudonym that can be

bureaucratically substantiated. With the right information criminals can set up bank accounts and numerous other relationships in the victim's name. The consequences of identity theft can be staggering. Victims are forced to spend time and money closing bank accounts and clearing credit records. The out-of-pocket expenses to clearing one's name can be enormous. Moreover, the debilitating consequences of identity theft can often take years to rectify. In the U.S., some past victims of identity theft are forced to carry documentation stating that they were victims of such a crime.⁵⁴

The highly publicized cases of identity theft in the U.S. sit as a stark reminder of what can happen when companies fail to provide adequate protections for the increasingly valuable information they hold about consumers. In January 2006, the Federal Trade Commission imposed \$15 million in fines and penalties against an American software company, ChoicePoint, as a result of a security breach that compromised the personal information of 145,000 U.S. residents. To date, nearly 800 of the exposed individuals have reported that some form of identity theft related crime has been committed against them.⁵⁵ Yet, despite the amount of negative publicity and public outcry, security breaches have been on the rise.⁵⁶ Since the ChoicePoint security breach in February of last year, security lapses have compromised the personal information of more than 50 million Americans.⁵⁷ According to *The Economist*, data theft in America resulted in losses totaling nearly \$50 billion in 2005 alone.⁵⁸ As a result of the proliferation of incidents of security lapses in the U.S., many states have pushed through tough laws that require companies to notify individuals in the event of a data breach shortly after it has occurred.

Disturbingly, incidences of identity theft are on the rise here in Canada.⁵⁹ This is why legislatures must take action to combat this crime from all angles. Amendments to the *Criminal Code* alone are not sufficient. Businesses that handle and deal in personal information must be held accountable for their security practices.

The only way true accountability can be achieved is by imposing upon every organization a legal obligation to report any data leak to the OPCC and to notify all individuals whose personal information has been the subject of a security breach. Furthermore, this notification should not be qualified or diluted in any way. Every time the security of someone's personal information is breached, it should be incumbent upon the organization charged with securing and protecting that information to inform the individual of the breach. This provides every individual the autonomy to make their own decision concerning what measures to take next. It should not be up to the organization to unilaterally decide the level of risk caused by the breach or the severity of the potential harm. When the personal information of an individual is involved, full disclosure must always be provided to the individual in order for him or her to make an informed decision as to how to proceed.

Some commentators have raised the concern that if organizations warn everyone about every breach, consumers may start to ignore the notices, which risks trivializing the effect of notifications over time.⁶⁰ This excuse simply does not hold water. There may of course be those consumers who do not pay attention to the warnings, but that is their prerogative. Taking away the right of all consumers to be notified of possible threats to their personal information simply because others may choose to ignore the warning does not make sense. All consumers must be

given full disclosure as to the breach, including the severity of the breach, the risks it poses and the potential for harm it represents. With this information in hand, consumers can then choose how to proceed.

Such arguments only serve the interests of those who do not want to reveal when they have not adequately protected the information with which they were entrusted. Allowing organizations to decide for themselves when they are obligated to inform consumers about a breach of their security systems puts these organizations in a dangerous conflict of interest with their customers. As such, it is essential that PIPEDA be amended to include a notification requirement that imposes a positive obligation on all organizations who handle personal information to notify all those affected by a breach (or suspected breach) each and every time.

In designing and drafting a “duty to notify” clause, PIAC strongly recommends emulating California’s privacy legislation in idea and wording. California’s *Security Breach Information Act*⁶¹ (formally known as Senate Bill 1386) came into effect on July 1, 2003. The law requires companies that do business in California or that have customers in the state to notify them promptly whenever their “unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” The statute only applies to “unencrypted personal information”, thus allowing the organization to avoid the notification requirements altogether if they chose to employ encryption technology to the personal information they maintain. The statute applies regardless of whether the computerized consumer records are maintained in or outside California. As long as a company conducts business in California and owns or licenses computerized data that includes “personal information” about residents, it has a legal obligation to notify its California consumers of security breaches to their personal information. The law further stipulates that companies failing to properly safeguard information or notify consumers of intrusions can be sued in civil court and face injunctions.

As such, SB 1386 provides a strong incentive for companies to adopt comprehensive security procedures, which include establishing a plan of action in the event of a security breach. Companies that fail to adequately secure their information face the cost of notification and the negative impact on image and consumer confidence associated with publicly disclosing a security breach. However, potentially the biggest repercussion for failure to comply with the law is that companies can face private actions for damages if they fail to notify consumers of a security breach, which could include class action lawsuits.

The law broadly defines “breach of the security of the system” as the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.” This definition excludes good faith acquisitions by an employee of the business, provided that the personal information is not used or subject to further unauthorized disclosure.⁶²

Notice may be provided in writing or electronically (provided certain conditions are met). If a company can demonstrate that the cost of providing notice would exceed \$250,000 or that the affected class of persons to be notified exceeds 500,000, or that the company does not have sufficient contact information, then it may instead use “substitute notice”. Substitute notice requires the following three actions: (1) email notice when the company has email addresses for

the subject persons; plus, (2) conspicuous posting of notice on the company's website, if it maintains one; plus (3) notification in a major state-wide media. Alternatively, a company that maintains its own notification procedures as part of an information security policy that is consistent with the timing requirements of the statute is deemed to be in compliance with the statutory requirements if it notifies the affected consumers in accordance with its policies.⁶³

Notification may also be delayed until the completion of any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. The law also allows for a delay of notification if a law enforcement agency determines that the notification will impede a criminal investigation.⁶⁴

These provisions contained in California's Bill 1386, are comprehensive in scope and impose a distinct obligation on California businesses to adopt and maintain comprehensive security procedures, which include a duty to notify every consumer affected by an actual or suspected security breach. Such legislation is not only an appropriate, but a *necessary* addition to PIPEDA, which at present has only vague admonitions in principle 4.7 to provide "security safeguards appropriate to the sensitivity of the information."

Recommendations:

PIAC recommends that PIPEDA be amended to include a similar notification requirement to that contained in California's Bill 1386. Specifically, PIPEDA should impose a legal "duty to notify" upon any organization in Canada that suffers a loss or theft of personal information they hold about Canadians. Furthermore, this duty should include any *actual* or *suspected* security breach, regardless of where the breach occurs. PIAC would also support the inclusion of an exception to the duty to notify for encrypted data - thereby giving organizations the choice of encrypting all personal data or having to abide by the notification requirements in the event of a breach. Similar to the California legislation, PIPEDA's notification provision should include provisions for alternate forms of notification, and the ability to impose heavy fines and exposure to civil actions for failure to notify in accordance with the law.

SUMMARY OF RECOMMENDATIONS

1. Powers of the Commissioner

PIAC strongly recommends that the powers of the Commissioner be amended to provide for an order-making power, along the lines of those in Québec, British Columbia and Alberta data protection legislation.

PIAC recommends that the OPCC adopt the policy of publicly naming organizations which have been found by the Privacy Commissioner to have violated PIPEDA. As a necessary component, PIAC further recommends that the OPCC adopt the policy of issuing full, published decisions of complaint investigations. It is however, imperative that complainants remain anonymous, both at the Commission level and at the Federal Court level.

Finally, the OPCC needs to put in place specific procedural rules for the collection and disclosure of evidence before the Commission. Additionally, an “agreed statement of facts” ought to be sought in each case before the Commissioner issues a final ruling, if the Commissioner does not otherwise obtain the power to make binding orders, which should imply a duty to make concrete factual findings with procedural safeguards for the parties to present and contest evidence.

2. Consent

PIAC recommends that PIPEDA be amended to clearly state that an “informed consent” standard is the appropriate measure to be applied throughout the Act, except where clear exceptions to this requirement are provided for.

PIAC further recommends strengthening the consent requirements under PIPEDA by including the following principles:

- Consent must be manifest - meaning that it is clear, certain and indisputable;
- Consent must be free - meaning that it must be given without compulsion;
- Consent must be enlightened - meaning that it must be precise, rigorous and specific;
- Consent is also given for a specified purpose; and
- Consent is a continuous process – meaning it is to be given for the length of time needed to achieve the purposes for which it was requested. The length of time will not necessarily be related to a number of days, months or years, but may refer to a specific event or situation

In addition, PIAC recommends that PIPEDA be amended to specifically prohibit the use of “blanket consent” statements as a means of obtaining consent.

3. *Duty to Notify*

PIAC recommends that PIPEDA be amended to include a similar notification requirement to that contained in California's Bill 1386. Specifically, PIPEDA should impose a legal "duty to notify" upon any organization in Canada that suffers a loss or theft of personal information they hold about Canadians. Furthermore, this duty should include any *actual* or *suspected* security breach, regardless of where the breach occurs. PIAC would also support the inclusion of an exception to the duty to notify for encrypted data - thereby giving organizations the choice of encrypting all personal data or having to abide by the notification requirements in the event of a breach.

Similar to the California legislation, PIPEDA's notification provision should include provisions for alternate forms of notification, and the ability to impose heavy fines and exposure to civil actions for failure to notify in accordance with the law.

¹ William A. Charnetski & Graeme Coffin, “Federal Privacy Legislation Leaves Much to be Considered” online: Torys LLP, Legal Analysis Papers <<http://www.torys.com/publications/pdf/AR2001-2T.pdf>>.

² Patricia J. Wilson & Michael Fekete, “Privacy Law in Canada” Osler, Hoskin & Harcourt LLP (june 2006), online: Doing Business in Canada, <<http://www.osler.com/resources.aspx?id=8686>>.

³ Sections 11-13.

⁴ Section 24.

⁵ Sections 18 and 12, respectively.

⁶ *Eastmond v. Canadian Pacific Railway*, [2004] F.C.J. No. 1043.

⁷ *L'Écuyer v. Aéroports de Montréal*, [2004] F.C.J. No. 1082.

⁸ Section 16.

⁹ 2003 FCT 705.

¹⁰ *Ibid.* at para. 39.

¹¹ *Englander v. Telus Communications Inc.*, [2004] F.C.J. No. 1935 (C.A.).

¹² *Ibid.* at para. 71.

¹³ *Ibid.* at para. 48.

¹⁴ For example, Mr. Englander was partially successful in his appeal the Federal Court of Appeal, however, he had been ordered to pay large legal costs to TELUS at the trial division level. If Mr. Englander had not acted as his own counsel and had the costs decision likewise overturned, he would have faced massive legal bills over a \$2 a month unlisted number service.

¹⁵ See “The Offices of the Information and Privacy Commissioners: The Merger and Related Issues” online: Department of Justice Canada <<http://www.justice.gc.ca/en/pl/p8.html>>.

¹⁶ *Ibid.*

¹⁷ *Ibid.*

¹⁸ The interdepartmental Task Force was mandated to review the *Access to Information Act* and its administration and to make recommendations to the government on how to improve access to government information for all Canadians. See the Access to Information Review Task Force website <www.atirtf-geai.gc.ca>.

¹⁹ *Access to Information Act*, R.S., 1985, c. A-1.

²⁰ *Supra* note 18.

²¹ *Ibid.*

²² Subsection 18(1).

²³ Subsection 18(2).

²⁴ See Audit of The Personal Information Management Practices of The Canada Border Services Agency Transborder Data Flows - Final Report, OPCC, online: <http://www.privcom.gc.ca/information/pub/ar-vr/cbsa_060620_e.pdf>.

²⁵ Subsection 11(2).

²⁶ See John Lawford, “Consumer Privacy under PIPEDA: How Are We Doing?” PIAC, (November 2004) at 12. Online: <http://www.piac.ca/privacy/report_consumer_privacy_under_pipeda_how_are_we_doing> [*Consumer Privacy Under PIPEDA*].

²⁷ *Ibid.* at 13.

²⁸ Subsections 20(1) and (2).

²⁹ *Consumer Privacy Under PIPEDA*, *supra* note 26 at 19.

³⁰ David Loukidelis, “Enforcing Private Sector Privacy – One Regulator’s Perspective” (Speech presented at *The Frontiers of Privacy & Security – New Challenges for a New Century Conference*, February 14, 2003). Online: <http://www.oipcbc.org/publications/speeches_presentations/CPIABspeech021203-2.pdf> [Loukidelis, “One Regulator’s Perspective”].

³¹ Subsections 13(1) and (3).

³² See Sarah Lysecki, “Does the Privacy Commissioner Need More Clout?” *itbusiness.ca* (August 9, 2006), online: <<http://www.itbusiness.ca/it/client/en/home/News.asp?id=40259>> [Lysecki, “Does the Privacy Commissioner Need More Clout?”].

³³ *Consumer Privacy Under PIPEDA*, *supra* note 26 at 9-10.

³⁴ Loukidelis, “One Regulator’s Perspective”, *supra* note 30.

³⁵ See “Letter to Privacy Commissioner of Canada” PIAC, November 16, 2004, online: <http://www.piac.ca/privacy/letter_to_privacy_commissioner_of_canada_1>.

³⁶ An “agreed statement of facts” practice has been suggested but has not been formally adopted by the OPCC. Assistant Privacy Commissioner Heather Black, in an interview, stated that the OPCC will be going back to organizations and saying “these are the facts that we are going to rely on.” It is not clear if the OPCC is also returning to the complainants to verify their version of the facts, but this was not done with the PIAC Bell Mobility and Bell ExpressVu complaints. See *ibid.* at 10.

³⁷ Office of the Privacy Commissioner of Canada, “PIPEDA Review Document: Protecting Privacy in an Intrusive World” (July, 2006), online: <http://www.privcom.gc.ca/information/pub/pipeda_review_060718_e.asp> [“PIPEDA Review Document”]

³⁸ Schedule 1, subclause 4.3.4.

³⁹ Schedule 1, subclause 4.3.5.

⁴⁰ Schedule 1, subclause 4.3.6.

⁴¹ *Ibid.*

⁴² Schedule 1, subclause 4.3.4.

⁴³ [2004] F.C.J.No. 1935 (CA); 2004 FCA 387.

⁴⁴ *Ibid.* at para. 56.

⁴⁵ CIPPIC, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (April 2006), online: <<http://www.cippic.ca/en/news/documents/May1-06/PIPEDAComplianceReport.pdf>>.

⁴⁶ *Ibid.* at 37.

⁴⁷ This list was adopted from that provided by The Commission d'accès à l'information du Québec. See online: <<http://www.cai.gouv.qc.ca/index-en.html>>.

⁴⁸ See CIPPIC, *Compliance with Canadian Data Protection Laws*, *supra* note 45. The results of CIPPIC's survey indicate that a significant portion of privacy policies fail the test of clarity. Moreover, the results indicate that the methods used by many online retailers to obtain consent from consumers do not meet the requirements for valid consent. See <http://www.cippic.ca/en/news/documents/May1-06/PIPEDAComplianceReport.pdf> for a complete report of the survey findings.

⁴⁹ See Advocis' response to the Privacy Commissioner of Canada PIPEDA Review Discussion Document, online: <http://www.advocis.ca/content/programs/advocacy/Sub-Privacy_Comm-se14-06.pdf>. For a complete report of the POLLARA survey findings, see: <www.advocis.ca/content/media/MR06/MR-feb15.html>.

⁵⁰ *Ibid.*

⁵¹ See CIPPIC, *Compliance with Canadian Data Protection Laws*, *supra* note 45 at 24-25.

⁵² See *Englander v. TELUS Inc.*, *supra* note 43 at para. 56.

⁵³ See CIPPIC, *On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship* (April 2006) at 47, online: <<http://www.cippic.ca/en/news/documents/May1-06/DatabrokerReport.pdf>>.

⁵⁴ See "Consumer Privacy Concerns: Identity Theft", The Canadian Privacy Institute, online: <<http://www.canadianprivacyinstitute.ca/consumer.html>>.

⁵⁵ Anthony D. Milewski Jr., "Compliance with California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide" 2 *Shidler J. L. Com. & Tech.* 19 (Apr. 14, 2006), online at: <<http://www.lctjournal.washington.edu/Vol2/a019Milewski.html>> [Milewski, "Compliance with California Privacy Laws"].

⁵⁶ For a chronology of data breaches reported since the ChoicePoint incident, see <<http://www.privacyrights.org/ar/ChronDataBreaches>>.

⁵⁷ Milewski, "Compliance with California Privacy Laws", *supra* note 55.

⁵⁸ *Ibid.* See also "Identity Theft: What's in a Name?" *The Economist* (3 May 2005) at 84.

⁵⁹ According to a telephone poll conducted by Ipsos Reid, 8% of Canadian adult who own credit cards indicate they have personally been a victim of identity theft – the fraudulent use of personal information for such purposes as making payments, opening bank accounts or obtaining loans. See "Canadians and Identity Theft: Concern on the Rise" Ipsos News Centre, <<http://www.ipsos-na.com/news/pressrelease.cfm?id=2826>>.

⁶⁰ See for example, Lysecki, "Does the Privacy Commissioner Need More Clout?", *supra* note 32.

⁶¹ S.B. 1386, *Security Breach Information Act*, Chapter 915, Stat. Cal., 2003.

⁶² “Bracing for the ‘Breach’ Law,” online: Symantec Enterprise Solutions <<http://www.enterprisesecurity.symantec.com/industry/finance/article.cfm?articleid=2715>> [“Bracing for the ‘Breach’ Law”].

⁶³ James F. Brelsford, “California Raises the Bar on Data Security and Privacy,” online: FindLaw <<http://www.findlaw.com/2003/Sep/30/133060.html>>.

⁶⁴ “Bracing for the ‘Breach’ Law”, *supra* note 62.

*** End of Document***