

**Submission to Industry Canada  
Considering the House of Commons Standing Committee on Access to  
Information, Privacy and Ethics' Report on  
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

January 15, 2008

## TABLE OF CONTENTS

<b><i>OVERVIEW</i></b> _____	<b>3</b>
<b><i>SCOPE OF COMMENTS</i></b> _____	<b>3</b>
<b>Select Issues Only</b> _____	<b>3</b>
<b><i>1. DATA BREACH NOTIFICATION</i></b> _____	<b>4</b>
Recommendations: _____	<b>6</b>
<b><i>2. CHILDREN'S PRIVACY</i></b> _____	<b>7</b>
a) <b>Consent Provisions do not Work with Children</b> _____	<b>7</b>
b) <b>The Myth of "Parental" Consent</b> _____	<b>8</b>
c) <b>A Different Approach</b> _____	<b>8</b>
Recommendations: _____	<b>9</b>
<b><i>3. "PUBLIC SAFETY" CONSENT EXEMPTIONS</i></b> _____	<b>9</b>
Recommendations: _____	<b>10</b>
<b><i>4. ENFORCEMENT</i></b> _____	<b>10</b>
Recommendations: _____	<b>11</b>
<b><i>SUMMARY OF RECOMMENDATIONS</i></b> _____	<b>11</b>

## OVERVIEW

The Public Interest Advocacy Centre (PIAC) appeared before the House of Commons Standing Committee on Access to Information, Privacy and Ethics when they reviewed the Personal Information Protection and Electronic Documents Act in December of 2006. PIAC appeared to give its views on how Parliament should 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.”

The Committee adopted certain positions in its report to Parliament after its hearings.<sup>1</sup> Industry Canada in turn has produced a paper commenting on the Committee's proposed changes to PIPEDA and instituted this consultation round on its own comments.<sup>2</sup>

PIAC therefore will comment on the issues raised both by the Committee's recommendations and Industry Canada's response, with a view to helping Industry Canada and other stakeholders appreciate the consumer issues and point of view raised by the review of this key legislation.

## SCOPE OF COMMENTS

### *Select Issues Only*

PIAC is unable to comment on all of the issues raised in the PIPEDA consultations thus far, whether by the Committee or Industry Canada. PIAC continues to experience financial constraints and notes that its comments are prepared without funding. Therefore we propose to comment, briefly, on the main issues that PIAC feels must be addressed in this review of PIPEDA, and which were overlooked or upon which the Committee or Industry Canada has taken a position that PIAC believes to be contrary to the consumer interest. Lack of comment on any other issue should not be seen as agreement with any position expressed by the Committee or Industry Canada. We have attached our written comments to the Committee, which deal with some of the same subjects and some additional ones. We also note PIAC's report on PIPEDA from 2004, which is available on PIAC's website and also outlines what we see as deficiencies in the present Act.<sup>3</sup>

---

<sup>1</sup> *STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA): Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, (May 2007). Online:

<http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/reports/rp2891060/ethirp04/ethirp04-e.pdf>

<sup>2</sup> Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics: Statutory Review of the Personal Information Protection and Electronic Documents Act. Online: [http://www.ic.gc.ca/epic/site/ic1.nsf/vwapj/ETHI-e.pdf/\\$file/ETHI-e.pdf](http://www.ic.gc.ca/epic/site/ic1.nsf/vwapj/ETHI-e.pdf/$file/ETHI-e.pdf)

<sup>3</sup> PIAC, *Consumer Privacy Under PIPEDA: How Are We Doing?* (November 2004). Online: <http://www.piac.ca/files/pipedareviewfinal.pdf>

PIAC therefore will be making comments on Data Breach Notification; Children's Privacy; Public Safety Consent Exemptions and Enforcement.

## 1. DATA BREACH NOTIFICATION

*Canada is slowly becoming singled out as the only jurisdiction with modern privacy laws but no positive requirement to force companies and governments to disclose to individuals when personal data is lost, stolen or otherwise improperly accessed. This review must conclude with a recommendation for legislation to ensure that companies and governments inform the public of data breaches. However, such a duty must be effective for consumers and citizens, it must be mandatory, it must be enforced.*

The present debate over data breach notification in the Committee and with Industry Canada appears to boil down to whether to copy provisions of other data breach notification laws, such as those contained in California's Bill 1386, or to produce a "made in Canada" solution. While it is true that with PIPEDA, Canada is fortunate to have a comprehensive privacy framework in which to situate any possible duty of notification, it is not true that PIPEDA can accomplish this task alone. If that were so, companies voluntarily would notify consumers upon data breaches occurring. We have seen from the Privacy Commissioner's own report that TJX (Winners) that the company notified law enforcement and banks prior to the Privacy Commissioner, and then eventually notified about 330 individuals in Canada by letter, however, although it is not clear from the report, it appears they did not do so in Canada until media reports of the incident, some two or three months after the initial discovery of the breach.

The basic problem with data breach notification that is not mandatory, not based on verifiable principles and left up to the company or government involved, is that there is a clear conflict of interest in allowing the organization that has had a breach be the one either to determine the scope or timing of the notification, or even whether to disclose it at all.

PIAC was not pleased that the Committee chose to recommend that the Privacy Commissioner of Canada review data breach reports from companies to determine if notification was appropriate. However, PIAC was not of the view that this would be too administratively burdensome for the Office of the Privacy Commissioner of Canada (OPCC). Rather, PIAC is concerned that the OPCC is not as well placed as the individual to determine what the appropriate action is for the individual. It should be remembered at all time that identity theft primarily affects the victim. The individual victim is better able to judge if a breach is serious to their personal circumstances (for example, he or she might be very vigilant if previously a victim of ID Theft).

PIAC therefore cannot support the Industry Canada position that data breach notification be left to the company or government entity involved to decide, for "certain breaches" (whatever that may mean – presumably "large" – again, whatever that may mean – breaches) based on a threshold of "high risk of significant harm to individuals or organizations". This standard is far, far, far too high and will mean that almost no breaches ever will be reported. It leaves the

conflict of interest squarely in place; even voluntary guidelines (backed up with the threat of ... what, exactly?) from the OPCC will not change this.

The dilemma faced by policymakers therefore is between a standard that requires notification “just to be sure” and that business will view as burdensome (although if they have no breaches, it will not be a burden) but that will allow individuals notice of the breach in most cases; and a standard that will encourage hiding all but the biggest spills (and that business will tout as the best solution for responsible companies) but that will leave consumers much as they are now: in the dark.

We cannot express the dilemma of the appropriate standard better than the observations found in a recent Study Conducted for the Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law, entitled “Security Breach Notification Laws: Views from Chief Security Officers”:

However, it is important to note the substantial difference between a standard that exempts notification when an organization finds that there is no risk versus a standard that requires notification only when an organization finds a risk of misuse. Both standards present obvious challenges. The former standard requires the investigation to prove a negative, and thus limits notice exemptions. The latter standard does not take into account the fact that organizations’ investigative abilities regarding who has accessed the data are limited, and that organizations may not always be able to make a determination that the data is or is not likely to result in misuse. Where this determination is available, notification should depend on the results of that determination. However, when the investigation cannot make a determination on risk, notification should be required, because these are the situations in which consumer efforts to monitor and catch identity theft incidents on their own are most needed.<sup>4</sup> [Emphasis added].

Yet even this formulation of the policy question assumes that there is an acceptable evaluation of “risk” by the organization losing the information. PIAC believes that there is an interest in the individual knowing that a company or government lost, misplaced or has had stolen (even temporarily) their personal information. Risk assessments obscure this interest.

Industry Canada and the Committee must cease in taking a paternalistic view of individuals’ right to control of their private information: it is not their place to determine whether a loss of that individual’s own private personal information is a “real” loss to them or exposes that individual to risk. That is the individual’s choice; that is the individual’s determination to make. If an individual’s autonomy over personal information is not recognized by Industry Canada or Parliament, the underlying rationale for privacy laws, and for personal privacy itself, is fatally undermined.

PIAC therefore urges Industry Canada to consider a model for data breach notification that is comprehensive in scope and imposes a distinct obligation on businesses and governments

---

<sup>4</sup> See Hoofnagle et al., *Security Breach Notification Laws: Views from Chief Security Officers* A Study Conducted for the Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law (December 2007). Online: [http://www.law.berkeley.edu/clinics/samuelsn/cso\\_study.pdf](http://www.law.berkeley.edu/clinics/samuelsn/cso_study.pdf)

to notify every consumer affected by *any* actual or suspected security breach. Even if an organization could prove there was no risk whatever to the individual, there should continue to be a public reporting of such an incident to a central registry. This central registry should store details and be publicly available (via a website) so that the general public, policymakers and researchers, as well as media and businesses and governments could analyze trends and identify problem areas.

Any breach notification requirement must be backed up by specific penalties that the OPCC should be empowered to seek against any companies or governments trying to hide a breach in the face of such a law. These administrative monetary penalties should be substantial enough to ensure compliance yet flexible enough to deal with specific circumstances. PIAC suggests a similar level as those earmarked for the proposed Do Not Call Registry, that is, up to \$15,000 **per breached record** for a large business and up to \$1,500 for a small business.

The “threshold” for reporting a data breach should be the simple fact of a breach of any of a prescribed list of personal data elements. Companies, and the OPCC should have little or no control at all of what is viewed by them as a serious or trivial breach. All should be reported. We therefore strongly object to the proposed standard in the Industry Canada consultation document and indeed to any risk-based assessment. Instead, the trigger should be loss, theft or other unauthorized access of personal information by a third party (that is, there would be a good faith exception for employees acting in the scope of their duties – this would not permit “snooping”, for example by hospital employees accessing a celebrity patient’s file) of certain defined data elements. This prescriptive list should also include a provision allowing for new identifying elements to be added; that is, any elements that could be used by, for example, a would-be identity thief that were not in the prescribed list, but which reasonably could be used to identify an individual, also should trigger a breach notification.

As for the mechanics of breach notification, what is key to consumers is an accurate, standardized breach notification method and content. CIPPIC has proposed a list of key details that should be included in all communications with consumers and with which PIAC agrees. Notification should be by a method that will reasonably bring the notice to the attention of the individual. Companies and government should not be permitted to contractually require customers or citizens to accept a particular form of notification (for example, a requirement to accept that e-mail is sufficient notice).

## **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. 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.

## 2. CHILDREN'S PRIVACY

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. 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. However, nowhere is this more of a challenge than with children and minors. As a result, more specific legislative requirements are needed to deal with children's privacy.

### ***a) Consent Provisions do not Work with Children***

***“These kids are nine and they are playing. They are not disclosing information for commercial purposes. Yet the kind of legislation that we have in place lets companies set up these kinds of environments and, through a very weak consent mechanism, capture that information and reconfigure it as a commercial commodity. (November 29, 2006)” – Quoted by the Committee from their PIPEDA Review hearings.***

Research work undertaken by Professor Val Steeves of the University of Ottawa reveals the extent to which children's online playgrounds are in essence target marketing data collection centres.<sup>5</sup> The work indicates that online games and other websites routinely gather Canadian children's personal information with little oversight and few rules.<sup>6</sup> This information is used to serve up a variety of advertisements to children – many of them age and subject matter inappropriate.<sup>7</sup>

Section 5(3) requires organizations to collect, use or disclose personal information only “for purposes that a reasonable person would consider appropriate in the circumstances.” PIAC submits that all secondary marketing to children based on this information gathering, usage and disclosure is an unreasonable use to a reasonable person. As Prof. Steeves notes, the children are at play; they do not appreciate the data gathering aspect of the websites is what pays for them.

That should be the end of the matter then; all such transactions can and should be challenged before the Privacy Commissioner. However, in practice, no individual complaints have, to our knowledge, been filed. This is hardly surprising, as the collection use and disclosures are buried in hard to read and long privacy policies that kids expect only their parents to read, if they show it to them at all before entering a website. As a result, consent from the kids most often simply doesn't exist.

---

<sup>5</sup> See, for example, <http://blog.privcom.gc.ca/index.php/2007/10/21/how-childrens-sites-see-your-kids-as-marketing-goldmines/> and video: <http://video.google.ca/videoplay?docid=7709702757763862786&hl=en-CA>

<sup>6</sup> Steeves, Valerie. (2006). *It's Not Child's Play: The Online Invasion of Children's Privacy*. University of Ottawa Law and Technology Journal 3(1): 169-188.

<sup>7</sup> Fielder, Anna, Will Gardner, Agnes Nairn, Jillian Pitt. (2007) fair game? Assessing commercial activity on children's favourite websites and online environments (National Consumer Council and Childnet International). Online: <http://www.childnet.com/publications/policy.aspx>

## **b) The Myth of “Parental” Consent**

### *Is parental consent really consent?*

Complicating matters is the fiction that parents exercise a parental consent with regard to kids’ personal information. This is very much the exception. Parents concerns tend to be towards paedophile-proofing, virus avoidance and stopping unauthorized buying by their kids. As a result, any “consent” assumed through this process is entirely that, assumed. It is extremely unlikely that there is any genuine informed consent to the real uses of children’s personal information by website operators and the advertising and other commercial interests that use this information.

The worst solution to adopt, therefore, is the U.S. COPPA-style screen requiring children of a certain age to get verifiable parental consent to continue with a website. This type of approach only will legitimize the fiction that parents have consented to all of the gathering and uses of their children’s personal information and effectively insulate the website operators and advertisers even from individual privacy complaints.

## **c) A Different Approach**

### *Make Secondary Targeted Marketing to Children Illegal*

A better solution is a prohibition on targeted secondary marketing to children. That is, codify the reasonable person standard that abhors the “Hansel and Gretel” approach of the data brokerage and advertising industries: children should not be lured to “play” at websites that are effectively used to gather their personal information for commercial purposes. If this approach is not taken, we shall see “cradle to grave” commercial profiling – a threat that is very close to existence.

PIAC suggests a new section 5(3.1) in PIPEDA that prohibits secondary marketing to children based on personal information gathered at websites or through mobile phones or otherwise. If this approach is not taken, we can only suggest codifying many of the Canadian Marketing Association’s rules regarding marketing to children.<sup>8</sup> The value in codifying the CMA rules (which do prohibit some marketing types and also contain stricter consent provisions) is that they then will bind non-members and be enforceable (provided PIPEDA is amended to add more enforcement mechanisms – as discussed below). Consideration should also be given, if the CMA’s approach is adopted, to flatly prohibiting certain types of advertisements and marketing from being targeted to children based on their personal information. These should include: gambling ads; dating; pornography; diet and weight loss;

---

<sup>8</sup> See Canadian Marketing Association, “Code of Ethics and Standards of Practice” (Effective January 1, 2007), sections K and L “Special Considerations in Marketing to Children/to Teenagers”. Online: <http://www.the-cma.org/PublicUploads/225849CodeofEthics06.pdf>

alcohol and tobacco; and “junk” food.<sup>9</sup> There should be no question these are inappropriate for minors and therefore unreasonable bases on which to gather and use personal information.

On the issue of data retention, it is also PIAC’s position that retention of data of children and minors gathered before any change in the law would have to be destroyed. If gathering of information for secondary marketing is prohibited, PIAC also believes that it is unreasonable that a child’s profile be used to target market them as an adult and that it should be illegal that any information gathered while he or she is a minor be used for such marketing upon their age of majority. That is, companies could not “stockpile” a child’s profile waiting for them to become legally an adult.

## **Recommendations:**

PIAC recommends PIPEDA be amended to prohibit secondary marketing to children based on personal information gathered while they are minors. Any data gathered during this period should not be available upon the minor reaching the age of majority.

## **3. “PUBLIC SAFETY” CONSENT EXEMPTIONS**

*Exemptions for “public safety” passed in the wake of the 9/11 terrorist attacks must be looked at critically. Companies should not act as agents of the state.*

PIAC believes that regarding “public safety” solely from the point of view of security and police authorities is unbalanced and unfair. The general public has an interest in the debate that may be satisfied by laws that protect civil liberties as well as provide for effective law enforcement.

The Committee’s findings on the “public safety” exemptions found in s. 7 of the Act, in particular, s. 7(1)(e) are striking. The Committee was of the opinion that the provision should be removed. PIAC is of the same view. As noted by the witnesses before the Committee, the provision allows companies, without a warrant, based on their own suspicions and nothing more, to gather information for the purposes of national security or policing.

Such a provision is certainly suspect from a constitutional point of view and rightly so. It is hard to fathom why a police service would be required to obtain a warrant to search for or intercept this information, but that a company can setup a collection scheme for a particular users and hand it over to the authorities without any judicial oversight.

PIAC also cautions against the “clarification” of s. 7(3)(c.1) to define “lawful authority” (which some companies, given the suspect constitutionality of subs. 7(1)(e) and other public safety consent exemptions in s. 7,<sup>10</sup> have used as an excuse to ask for a judicial warrant before releasing

---

<sup>9</sup> See Fielder et al., *Fair Game?*, *supra*.

<sup>10</sup> PIAC has similar concerns with subss. 7(3)(c.1) and 7(3)(d).

information) as this risks removing a way for companies to insist upon a warrant, even in the case of subs. 7(1)(e). If s. 7(1)(e) is not removed, then no clarification of “lawful authority” should be undertaken without a parallel “clarification” that any of the public safety exemptions in s. 7 cannot be used to otherwise avoid a warrant requirement or circumvent the law on constitutional searches and seizures.

## **Recommendations:**

PIAC recommends that s. 7(1)(e) of PIPEDA be removed and other “public safety” exemptions be examined to ensure they cannot be used to otherwise avoid a warrant requirement or circumvent the law on constitutional searches and seizures (and that PIPEDA be amended to ensure this, if necessary).

## **4. ENFORCEMENT**

### *PIPEDA is a paper tiger.*

There are several important reasons why the existing ombudsman model is ineffective at protecting the privacy rights of Canadians. These PIAC detailed in its submissions to the Committee. They include: Lack of Order-making power; Under-utilization of Current Enforcement Tools; Refusal to Name Offenders; and Inadequate Findings Summaries. PIAC will not restate all of the problems in detail. However, we note that if the present review adds any mandatory breach notification requirements, it will be essential that the OPCC be given the power to enforce compliance. If this is done, it will be the only enforcement power as such possessed by the Privacy Commissioner. However, it will be absolutely necessary to possess such power or the breach notification requirements will be widely ignored, as have other basic PIPEDA requirements.

PIAC holds out the promise of privacy rights to Canadians but delivers very little.<sup>11</sup> This is in part due the fact that the role and functions of the Office of the Privacy Commissioner are incomplete and there is frankly no incentive for companies to comply with findings of the Commissioner, which are only persuasive. The OPCC inexplicably acquiesces in its lack of power and appears misled by its faith in its persuasive powers. The unfortunate result is that only persons in the three provinces with privacy commissioners who have order making powers have any real prospect of the enforcement of an order to rectify a privacy problem.

PIAC notes with alarm that the OPCC appears to have abandoned its previous commitment even to publish its findings. At the least, an amendment to PIPEDA requiring the OPCC to publish its findings, in full, while naming respondents, is required, if only for the outside possibility that individual consumers, if not the OPCC, can discipline the market into privacy protection.

---

<sup>11</sup> See PIAC, *Consumer Privacy Under PIPEDA: How Are We Doing?* *supra*.

## 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. Since this appears unlikely given the OPCC's resistance to order making power, an amendment to PIPEDA requiring the OPCC to publish its findings, in full, while naming respondents, is required. In addition, if any mandatory breach notification sections are added to the Act, the OPCC will be required to have the power to impose significant AMPs.

## SUMMARY OF RECOMMENDATIONS

### *1. Data Breach Notification*

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. 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.

### *2. Children's Privacy*

PIAC recommends PIPEDA be amended to prohibit secondary marketing to children based on personal information gathered while they are minors. Any data gathered during this period should not be available upon the minor reaching the age of majority.

### *3. Public Safety Consent Exemptions*

PIAC recommends that s. 7(1)(e) of PIPEDA be removed and other "public safety" exemptions be examined to ensure they cannot be used to otherwise avoid a warrant requirement or circumvent the law on constitutional searches and seizures (and that PIPEDA be amended to ensure this, if necessary).

### *4. Enforcement*

PIAC recommends that PIPEDA be amended to provide the Privacy Commissioner of Canada with order-making power. Failing this, an amendment to PIPEDA requiring the OPCC to publish its findings, in full, while naming respondents, is required. In addition, if any mandatory breach notification sections are added to the Act, the OPCC will be required to have the power to impose significant AMPs.