Submission to the Special Committee to Review the *Personal Information Protection Act*

February 29, 2008

Darrell Evans
BC Freedom of Information and Privacy Association
BC Civil Liberties Association

The BC Freedom of Information and Privacy Association and the B.C. Civil Liberties Association frequently work together on privacy issues. This is the joint submission of our two organizations to the Special Committee to Review the *Personal Information Protection Act.*

The BC Freedom of Information and Privacy Association (FIPA) is a non-profit society established in 1991 for the purpose of advancing freedom of information, open and accountable government, and privacy rights in Canada. We serve a wide variety of individuals and organizations through programs of public education, legal aid, research, public interest advocacy and law reform.

The B.C. Civil Liberties Association was established in 1962 and is the oldest and most active civil liberties group in Canada. We are a group of citizens who volunteer our energy and talents to preserve, defend, maintain and extend civil liberties and human rights in British Columbia and across Canada.

First, we would like to reiterate our opinion that the *Personal Information Protection Act* (PIPA) is a very good piece of privacy legislation. In fact, it was a huge breakthrough for privacy rights in the provinces outside Quebec, and improved on its federal counterpart, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in many ways.

BC showed strong leadership among the provinces in moving forward in 2001 with a private-sector privacy act that has real teeth. For this, great credit is due to then Minister of Management Services, Sandy Santori, and to Chris Norman and Sharon Plater, the officials who conducted the public consultation process and led the development of the legislation.

PIPA was the product of a consultation process that was very thorough and quite fair...even though we estimate that about 50 business organizations were consulted for every privacy advocate. The consultations lasted a year, and FIPA and BCCLA participated in at least 12 meetings. Over six months, we and the government officials examined and debated progressive drafts section by section and almost line by line. A transformation began to occur, and after six months, the bill had turned into what we consider to be a serious privacy bill.

The Merits of BC's *Personal Information Protection Act*

First, we would like to describe what we like most about the PIPA. Our "LIKES" outweigh our "DISLIKES":

- THE LEGISLATION IS CLEARLY DRAFTED AND SIMPLER THAN THE PIPEDA
- IT COVERS THE ENTIRE PROVINCIAL PRIVATE SECTOR, INCLUDING NON-PROFIT ORGANIZATIONS (not just information used for commercial purposes like PIPEDA).
- IT INCLUDES OVERSIGHT AND ENFORCEMENT BY A COMMISSIONER WITH ORDER-MAKING POWER
- THE RIGHT OF CONSENT IS AT THE HEART OF THE ACT (as it should be.)
- THE EXCEPTIONS TO THE CONSENT PRINCIPLE ARE FAIRLY LIMITED
- THE PURPOSES FOR COLLECTION, USE AND DISCLOSURE MUST BE SPECIFIED AND MUST BE REASONABLE
- CONSENT MUST BE EXPLICIT IF INFORMATION IS SENSITIVE (Not 'implied' following one's failure to exercise an "opt-out".)
- THERE IS AN EXCEPTION ALLOWING USE OF PERSONAL INFORMATION FOR RESEARCH WITHOUT CONSENT, BUT IT IS FAIRLY NARROW
- THE ACCESS TO INFORMATION PROVISIONS ARE REASONABLE
    - Only a "Minimal" fee may be charged for copies of all your personal information. This is better than a "reasonable" fee as in PIPEDA.
    - There is no charge for access to one's own employee information
- PIPA CONTAINS GOOD WHISTLEBLOWER PROTECTION (as does PIPEDA)

And finally,

- THERE ARE STRONG PENALTIES FOR OFFENSES...such as:
    - The use of deception or coercion to obtain information
    - Disposing of PI to evade an access request
    - Obstructing the commissioner or failing to comply with an order
    - Contravening whistleblower protections
    - Fines for offenses are up to $10,000 for individuals and $100,000 for organizations, and an individual may also sue for damages for actual harm
    - An individual may sue for damages for actual harm caused.

How should PIPA be improved?

In this submission, we will focus on the six main ways we think PIPA should be improved. They are:

1. **The broadness of PIPA's exceptions to the requirement to obtain informed consent for the collection, use and disclosure of personal information. These exceptions should be narrowed.**
2. **Weak requirements for organizations to be open with the public about their privacy policies and practices.**
3. **Unfair limits to individuals' rights to have access to their own personal information and correct the information when it is wrong.**
4. **Inadequate offences and penalties for breaches of the act.**
5. **Inadequate protections for our personal information when it leaves Canada or is placed in the hands of organizations subject to foreign laws.**
6. **The lack of a requirement to inform the public when privacy or security breaches place our information at risk.**

We will now deal with these aspects of PIPA in more detail.

1. THE BROADNESS OF PIPA'S EXCEPTIONS TO THE PRINCIPLE OF CONSENT

The heart of privacy protection laws is the "Consent" principle: that "The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate."

This is Principle 1 of the Canadian Standards Association's *Model Code for the Protection of Personal Information*, which is entrenched in the federal PIPEDA and is a core principle of PIPA as well.

All privacy laws include some exceptions to their consent requirements, and as always with legislation, "the devil is in the details": if exceptions to the rules become too broad, a ***privacy*** law can easily become a ***disclosure*** law.

The exceptions to the consent requirements in PIPA are fairly limited, but they are too broad in several respects:

Section 8 – Implicit consent

In the case of implied or "deemed consent" as seen in section 8 (1), the consent is valid only if the purpose for the collection, use or disclosure "would be considered obvious to a reasonable person". However, what is seen as "obvious" to an organization may well not be considered so by a consumer.

In particular, organizations have often considered their intention to use personal information for secondary marketing purposes as obvious and reasonable and therefore not needing explicit consent, whereas a number of studies indicate that consumers feel otherwise.

For example, a study commissioned by Ontario's Public Interest Advocacy Centre showed that a large majority of Canadians (82%) want to be asked for their permission before a company uses their personal information to build a profile on them for the purposes of marketing new products and services.[1]

The same survey noted that 87% of Canadians polled feel it is important that banks obtain their positive consent prior to sharing their personal information with bank affiliates.

If there is any doubt at all whether an intended purpose would be obvious to a reasonable person, it should be spelled out and easily available in a notice.

Negative option consent

PIPA allows an individual's consent to be implied if they fail to exercise an "opt-out" option, described in section 8 as follows:

> 8 (3) An organization may collect, use or disclose personal information about an individual for specified purposes if
>
> (a) the organization provides the individual with a notice, in a form the individual can reasonably be considered to understand, that it intends to collect, use or disclose the individual's personal information for those purposes,
>
> (b) the organization gives the individual a reasonable opportunity to decline within a reasonable time to have his or her personal information collected, used or disclosed for those purposes,
>
> (c) the individual does not decline, within the time allowed under paragraph (b), the proposed collection, use or disclosure, and
>
> (d) the collection, use or disclosure of personal information is reasonable having regard to the sensitivity of the personal information in the circumstances.

This process is also known as "negative option" consent.

One problem with this approach stems from the lack of rigor in PIPA's notification requirements as found in section 10. This weakness will be described more fully below under "Openness of privacy policies and practices", but in a nutshell, *PIPA does not require an organization to make available a clear, comprehensive, and easily accessible description of its policies and procedures regarding the collection, use and disclosure of personal information, including all the purposes for which it collects personal information.*

Without such explicit notification, an individual cannot be considered to have given informed consent to an organization's practices or to have been offered a legitimate opt-out option.

---

[1] 2001 survey of Canadian opinion by **Ekos** for the Public Interest Advocacy Centre http://www.piac.ca/Direct%20marketing%20conclusions.pdf

All of us are familiar with inadequate opt-out offers. Their features include:

- Failure to adequately bring an opt-out offer to the attention of the individual so as to ensure awareness;
- Failure to provide adequately detailed information about the practices in question (such as the use of customer data for secondary marketing purposes) so that the consumer can fully appreciate the extent and purpose of uses and sharing to which they are consenting;
- Failure to provide the relevant information in clear, plain language such that the ordinary consumer can easily understand what they are being assumed to have consented to; and
- Failure to provide customers with a method of opting-out that can be executed immediately, easily, and at minimal effort and cost.

A legitimate opt-out should not require the use of a computer, which many consumers do not have; should involve minimal effort on the part of the consumer (e.g., should not require the consumer to write a letter and mail it to a postal address), and should be able to be exercised at minimal cost (e.g., should not require a long distance telephone call).

Recommendation 1:

That PIPA be amended to provide that

a) If there is any doubt at all whether an intended purpose would be obvious to a reasonable person, consent should not be implied; rather, the purpose should be spelled out in a clear and readily available notice.

b) If necessary to resolve conflicting interpretations of what purposes are obvious to a reasonable person, PIPA or its regulations should be elaborated to further define the circumstances in which consent may be implied.

c) If opt-out or negative option consent is permitted, it should only be permitted in limited, specified circumstances, and only where specific conditions have been met. Those conditions should require that the negative option
    - is effectively brought to the individual's attention,
    - is clearly worded
    - provides sufficient detail for the consumer to make an informed choice, and
    - is easy to execute at minimal cost.

2. OPENNESS OF PRIVACY POLICIES AND PRACTICES

Principle 8 of Canada's National Standard *Model Code for the Protection of Personal Information* is "Openness"– meaning the requirement for organizations to be completely open about their policies and practices with regard to personal information. Only when there is openness can the public give truly informed consent to the collection, use and disclosure of their personal information.

This is an area in which PIPA has been found wanting.

Citizens have filed formal complaints with FIPA and the Information and Privacy Commissioner stating that some organizations have been less than open about their privacy policies and practices, but weak standards and a lack of clarity in PIPA concerning openness requirements, together with timid enforcement by the Commissioner's office, have in some cases prevented citizens from receiving a written privacy policy and a thorough description of policies and practices.

The act's language should be clarified and strengthened so that it at least matches the standards of the *Model Code.*

The "Openness Principle" of the *Model Code* as incorporated in PIPEDA, states:

> **4.8 Principle 8 – Openness**
>
> An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
>
> 4.8.1
>
> Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.
>
> 4.8.2
>
> The information made available shall include
>
> a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
>
> (b) the means of gaining access to personal information held by the organization;
>
> (c) a description of the type of personal information held by the organization, including a general account of its use;
>
> (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
>
> e) what personal information is made available to related organizations (e.g., subsidiaries).
>
> 4.8.3
>
> An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

In contrast, the relevant sections of PIPA are as follow:

> **Required notification for collection of personal information**
>
> **10** (1) On or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing
>
> (a) the purposes for the collection of the information, and
>
> (b) on request by the individual, the position name or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about the collection.
>
> **Policies and practices**
>
> **5** An organization must
>
> (a) develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act,
>
> (b) develop a process to respond to complaints that may arise respecting the application of this Act, and
>
> (c) make information available on request about
>
> (i) the policies and practices referred to in paragraph (a), and
>
> (ii) the complaint process referred to in paragraph (b).
>
> **Implicit consent**
>
> **8** (1) An individual is deemed to consent to the collection, use or disclosure of personal information by an organization for a purpose if
>
> (a) at the time the consent is deemed to be given, the purpose would be considered to be obvious to a reasonable person, and
>
> (b) the individual voluntarily provides the personal information to the organization for that purpose.
>
> …
>
> (3) An organization may collect, use or disclose personal information about an individual for specified purposes if
>
> (a) the organization provides the individual with a notice, in a form the individual can reasonably be considered to understand, that it intends to collect, use or disclose the individual's personal information for those purposes,
>
> (b) the organization gives the individual a reasonable opportunity to decline within a reasonable time to have his or her personal information collected, used or disclosed for those purposes,
>
> (c) the individual does not decline, within the time allowed under paragraph (b), the proposed collection, use or disclosure, and

> (d) the collection, use or disclosure of personal information is reasonable having regard to the sensitivity of the personal information in the circumstances.

Here are some of the shortcomings of the above sections of PIPA with regard to the "Openness" principle:

Section 10 (1), Required notification :

a) The information required to be provided to the individual falls far short of the standard required by PIPEDA (See 4.8.2 on page 6).

b) Information adequate to ensuring informed consent cannot be delivered verbally as permitted by PIPA.

c) An individual should not have to request the contact information necessary to inquire about the collection, use or disclosure of information. Individuals should be routinely and immediately informed of contact information and where all the other information necessary for them to grant informed consent is available.

Section 5, Policies and practices:

Section 5 (c) is seriously inadequate in specifying the quantity, quality and nature of information organizations must make available about their information policies and practices and their process for responding to complaints.

- First, it requires only that organizations "make information available on request". As stated above, such information should be readily available as a matter of routine practice.
- Second, it requires only that information "about" organizational policies and practices and their complaint process be made available.

It is the latter failing that has caused the most difficulties and unfairness to complainants. Organizations have been able to provide very limited information about policies and practices, rather than the comprehensive information necessary to secure true informed consent. The openness principle is not upheld unless an organization's privacy policy, practices and complaint process are clear, comprehensive and easily accessible. All the purposes, uses and disclosures of personal information intended by the organization should be made public.

Section 8, Implicit consent:

The openness principle is especially important where an organization intends to either imply that consent is obvious or employ "negative option" consent (See above).

In the case of negative option consent, PIPA requires that purposes must be "specified" and notice provided "in a form the individual can reasonably be considered to understand". We refer the reader once again to the weaknesses detailed above regarding required notification.

Recommendation 2:

a) That the "Openness Principles" of the Model Code for the Protection of Personal Information be incorporated more effectively into PIPA. The openness principle requires that an organization's privacy policy, practices and complaint process be clear, comprehensive and easily accessible.

b) That, on or before collecting personal information from an individual, an organization should be required to provide the individual with or refer them to the organization's written privacy policy.

c) That all the purposes, uses and disclosures of personal information intended by the organization should be made public as part of the "Required notification for collection of personal information".

3. LIMITS TO RIGHTS OF ACCESS AND CORRECTION

People must have effective rights of access to their personal information and to demand that it be corrected where it is false. There is a problem with the relevant sections of PIPA, sections 23 and 24.

Principle 9 of the *Model Code for the Protection of Personal Information* states:

> **Individual Access**
>
> Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Section 23, Access to personal information

Section 23 of PIPA, "Access to Personal Information", generally upholds this principle. However, there is a major exception that is not paralleled in PIPA. S. 23(4) (d) of PIPA requires that an organization must not disclose personal and other information to an individual if "…the disclosure would reveal the identity of an individual who has provided personal information about another individual and the individual providing the personal information does not consent to disclosure of his or her identity."

This exception is excessive and unfair. It would prevent individuals from obtaining access to vital information and opinions about themselves if it would reveal the identity of individuals who provided the information – even if the information were seriously in error or provided in bad faith. It could prevent the requesters from understanding and having the opportunity to correct information about themselves that may be used to make important decisions about them.

We understand that access to one's own information should sometimes be limited in order to protect a third party who is a source of information. However, we think this should apply only where a clear case can be made that the third party or another specific interest will be harmed, and where the potential of harm is sufficiently serious to merit overriding an individual's normal right of access.

Recommendation 3:

Amend section 23(4) (d) of PIPA so that an individual may be denied access to their personal information only where a clear case can be made that the third party or another specific interest will be harmed, and where the potential of harm is sufficiently serious to merit overriding an individual's normal right of access.

Section 24, Right to request correction of personal information

When an organization refuses to correct what a complainant alleges to be an error or omission in their personal information, the organization is required under s. 24 (3) to annotate the personal information under its control with the correction that was requested but not made.

There has often been disagreement between complainants and organizations over the nature, prominence and placement of annotations that should be required under s. 24(3). We recommend that PIPA be amended so as to require that such notations be "easily apparent". This may not seem at first glance to be sufficiently important to warrant an amendment, but we can assure the members of the Special Committee that it is extremely important to individuals about whom critical decisions may be made based on the contents of a file.

Recommendation 4:

That when a correction is requested under s. 24 of PIPA, the annotation of a correction that was requested but not made must be added to the personal information of the complainant in such a way and in such a location as to be easily apparent when the information is examined by any potential viewer.

4. OFFENCES AND PENALTIES

Failure to adequately protect personal information should be an offence

The public is very concerned about the security of their personal information, particularly in cases where it makes them vulnerable to fraud or identity theft. In PIPA, the form of safeguards that may be considered "reasonable" depends upon the sensitivity of the information: the more sensitive the information, the higher the level of protection required.

However, currently under PIPA, if an organization fails to take reasonable security precautions to safeguard personal information, there is no offence or penalty that a court can assess.

Recommendation 5:

That an offense be added to PIPA section 56, "Offences and Penalties", for failure to take reasonable security precautions to safeguard personal information as required by section 34, "Protection of personal information".

Destruction, alteration, falsification, or concealment of evidentiary records should be an offence

It is currently an offence under PIPA to obstruct the Information and Privacy Commissioner in the course of the performance of his duties under the Act. We think there should also be a specific offence for the destruction, alteration, falsification, or concealment of evidentiary records during an investigation or inquiry by the Commissioner.

Recommendation 6:

That an offense be added to PIPA section 56, "Offences and Penalties", for disposing of, altering, falsifying, concealing, or destroying evidence during an investigation or inquiry by the Commissioner

5. TRANSBORDER DATA FLOWS: WHEN PERSONAL INFORMATION LEAVES CANADA

As a society, Canadians have worked hard to entrench privacy rights in the law of our land. The result is that privacy laws now exist at all levels of government – nationally, in all the provinces and territories, and in the private sector. The significance of this progressive expansion of rights is enormous. It should be better appreciated and better understood.

British Columbia took some leadership in this expansion, first by enacting and then by significantly reinforcing, a strong private-sector privacy law.

However, there has always been an annoying global fly in our national ointment: We can pass strong privacy laws in Canada, but what happens when our personal information leaves the country or in other ways becomes subject to foreign laws?

The need to provide international protection for personal information is demonstrated by the fact that the federal PIPEDA was enacted for the express purpose of bringing Canadian law into line with the privacy protection laws of the European Union. This helped Canada deal with a legislative gap between ourselves and the EU that otherwise might have become a trade barrier.

The essential question is "In a Global economic environment where personal information moves everywhere electronically, and information management is also globalized, how can we ensure that Canadians' information does not become subject to a lesser standard of privacy protection than that provided by Canadian law, regardless of who has access to or control of it?

Foreign-owned corporations are subject to the laws of the countries in which they operate, but they are also subject to the laws of their home country, regardless of where they are operating. There is a great disparity between the Canadian approach to privacy protection and that of many other countries, including our largest trading partner, the United States.

BC's Information and Privacy Commissioner noted the disparity between Canadian and American approaches to privacy and stated that "As a result of this disparity,

Canadian personal information flowing across the border into the US does not always enjoy the same standards for protection that we have come to expect here."[2]

The Commissioner also concluded that a foreign-owned contractor to a Canadian company could be compelled by the laws of its native country (e.g., for an American-owned company, the USA Patriot Act) to collect, use or disclose the personal information of Canadians in ways not allowed by PIPA.

The Commissioner grappled with this problem and how to solve it in 2004. He provided his assessment of the privacy problems inherent in trans-border data flows and proposed a reasonable set of solutions in a report called *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*.

The Commissioner's recommendations are directed at the management of the BC government's data holdings, but some are also relevant to the management of information in BC's private sector.

Are there absolute ways to protect our personal information, short of forbidding Canadian organizations from sending information across borders or contracting to foreign-owned firms? The Commissioner concluded there definitely are not.

Should we then forbid private-sector organizations from sending Canadians' personal information across borders or contracting its management to foreign-owned firms? The first would be impossible; the second would require a breathtaking iconoclasm toward globalization that is highly unlikely in the British Columbia of today.

Both public- and private-sector organizations have told us that it is almost impossible to avoid sharing personal information, and in some cases contracting its management, to companies subject to foreign laws that provide inferior privacy protection. Recognizing this, we hope that the modest recommendations below will at least mitigate the problems that could arise from disparate laws.

Accountability for personal information practices

An organization should not be allowed to "contract out" of its PIPA requirements, and it must be responsible for maintaining these standards even if it chooses to send data across borders.

PIPEDA deals with this issue by incorporating Principle 1 of the *Model Code for the Protection of Personal Information*, "Accountability", which states:

> **Principle 1 – Accountability**
>
> **4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

The only comparable reference in PIPA to responsibility for personal information is section 4 (2), which states

[2] *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*, p13.

> An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization.

This is not sufficient. PIPA should expressly state that

- where an organization governed by PIPA engages the services of a person by contract or otherwise, the organization is responsible for that person's compliance with the Act with respect to those services; and
- that organizations continue to be accountable for the security of personal information when it is transferred to a service provider for processing – regardless of where in the world that service provider operates.

Recommendation 7

That an amendment be added to PIPA explicitly stating

a) That organizations are responsible for the personal information in their custody or control, including information that has been transferred to a third party for processing;

b) That organizations shall use contractual or other means to ensure compliance with the Act and provide a comparable level of protection while the information is being processed by a third party, regardless of where the third party is located;

c) That a contractor is required to notify the organization of any subpoena, warrant, order, demand or request made by a foreign court or other foreign authority for the disclosure of personal information to which PIPA applies; and

d) That a contractor is required to notify the organization of any unauthorized disclosure of personal information under PIPA.

Require organizations to inform individuals of trans-border flows of their personal information

The Special Committee that reviewed Alberta's *Personal Information Protection Act* made its final report in November 2007. We would like to include part of that report here and adopt its recommendation:

> **Processing personal information outside Canada**
>
> The Committee heard that organizations and individuals are concerned that PIPA does not provide adequate protection for personal information transferred to a third party for processing or storage outside Canada…
>
> PIPEDA applies where personal information is transferred across a provincial border in the course of a commercial activity. PIPEDA expressly requires an organization to use contractual or other means to provide a comparable level of protection while information is being processed by a third party. The Committee heard that the federal Privacy Commissioner has determined that an organization is not obliged under PIPEDA to obtain consent or to provide clients with the ability to "opt out" of having their personal

information transferred to a service provider. However, the organization must provide notice of third-party processing to clients. It is unclear whether the Alberta Information and Privacy Commissioner would follow the federal Commissioner's findings in this matter.

Notice of and consent to transfer personal information outside Canada

PIPA generally requires an organization to obtain consent for the collection, use or disclosure of personal information. When collecting directly from an individual, an organization must provide notification to the individual, before or at the time of collection, of the purpose of the collection and the name of a person who can answer questions about the collection. There is currently no requirement to notify an individual of a transfer of personal information outside Canada…

The Committee believed there was a need to strengthen consumer protection and clarify existing obligations of organizations under PIPA. The Committee understood that requiring notification for third-party processing might require businesses to commit additional resources to their communication processes, but strongly believed that individuals have the right to know that their personal information is being sent outside the country. The Committee unanimously recommended:

1 That the Act be amended to require organizations to notify individuals when they will be transferring the individuals' personal information to a third-party service provider outside Canada.

Recommendation 7

That PIPA be amended to require organizations to notify individuals when they will be transferring the individuals' personal information to a third-party service provider outside Canada.

6. DATA SECURITY BREACH NOTIFICATION

The last few years have seen an abrupt rise in the number of large-scale security breaches involving the sensitive personal information of millions of people, and a large rise in the number of people who have become victims of the crimes of identity theft and identity fraud.

A general lack of transparency regarding shoddy corporate information practices, data security breaches and identity fraud has undoubtedly allowed poor practices to continue. Neither governments nor corporations have been eager to publicize such failings, as both sectors have a huge stake in maintaining public confidence in electronic commerce. But without a concerted effort to improve openness and data protection, public trust will be damaged and may actually decline.

Identity fraud offers low risks and high rewards for its perpetrators, combined with potentially high costs and devastating personal consequences for its victims.[3]

In 2005, Phonebusters, a Canadian organization which studies and reports on identity theft, collects data, educates the public and assists Canadian and U.S. law enforcement agencies in consumer fraud cases, received over 12,000 complaints

[3] FIPA and BCCLA wish to credit the Canadian Internet Policy and Public Interest Clinic (CIPPIC) for much of the content of this section. Reports cited include *Approaches to Security Breach Notification: A White Paper* (January 9, 2007) and *CIPPIC Submission to Industry Canada re: PIPEDA reform issues* (January 15, 2008). See www.cippic.ca

from victims of identity theft. The associated losses were an estimated $8.6 million. By October 2006, Phonebusters had received fewer complaints than in the previous year, but total losses had risen to almost $15 million.[4]

In the U.S., identity theft has topped the Federal Trade Commission's (FTC) list of consumer complaints for years. In 2004, the FTC received 246,570 identity theft complaints and in 2005, 255,565 complaints were recorded. Between 2003 and 2005, approximately 9 million Americans were victims of identity theft annually. In 2005, losses to victims and businesses were an estimated $56.6 billion.

Recognizing that individuals need to know when their personal information has been put at risk in order to mitigate potential identity fraud damages, most states in the U.S. now have laws requiring that organizations notify affected individuals when a security breach exposes their personal information to unauthorized access.

In contrast, neither PIPEDA nor PIPA include an explicit security breach notification requirement.

Sixty-eight percent (68%) of respondents to a recent Canadian survey felt that individuals and government agencies should be notified in the event of a data security breach.[5]

Due to growing public concern, the Canadian government has finally stepped up to the plate on security breach notification. Last year, a House of Commons committee recommended that PIPEDA be amended to require corporations to notify individuals of security breaches that expose their personal information to potential misuse.

As a result, the government of Canada is moving toward enacting an amendment to PIPEDA that requires organizations to disclose security breaches. Industry Canada is leading the national consultation on breach notification. As stated in the Canada Gazette notice, a statutory requirement for notification of data breaches

> "…[I]s an important component of a comprehensive strategy to address the growing problem of identity theft.…Ultimately, a requirement for data breach notification should encourage organizations to implement more effective security measures for the protection of personal information, while enabling consumers to better protect themselves from identity theft when a breach does occur.

It seems that an amendment to PIPEDA is certain; only the manner of disclosure is a subject of debate. Will it be a rigorous process that informs and empowers the public, or a conservative approach with weak enforcement and a great deal of discretion about reporting left to organizations?

FIPA and BCCLA have endorsed the approach to data security breach notification put forward by the Canadian Internet Policy and Public Interest Clinic (CIPPIC).

CIPPIC made a submission on November 28, 2006 to the House of Commons Standing Committee on Access to Information, Privacy and Ethics in its review of the *Personal*

---

[4] The Canadian Anti-Fraud Call Centre (Phonebusters), Monthly Summary Report (October 2006)
[5] EKOS Research Associates, *Identity Theft & Identity Management: Looking Through the Eyes of the Canadian Public*, (Paper presented to the 7th Annual Privacy and Security Workshop, Toronto, 3 November 2006).

Information Protection and Electronic Documents Act. We offer the following recommendations CIPPIC made to the Commons committee as equally applicable to PIPA.

Recommendation 8

That the following recommendations made to the House of Commons concerning data breach notification be adopted by the BC Special Committee to review the *Personal Information Protection Act.*

Breach Notification Trigger and Risk Assessment

Notification should be required when designated personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency should not trigger the notification requirement, provided that the personal information is not used or subject to further unauthorized disclosure."

We recommend adoption of the threshold applied in California and many other states in the U.S.: acquisition, or reasonable belief of acquisition, by an unauthorized person. This standard is higher than mere "access by an unauthorized person", but lower than standards that incorporate a "risk of identity fraud" element. We believe that, together with the proposed definitions below, it properly balances the competing interests at play.

The trigger for notification should be based on an objective test applied by organizations and subject to review by the applicable Privacy Commissioner. The test should be designed to avoid notification obligations where the breach does not expose individuals to a real risk of identity theft, but to apply in all situations where such a risk is created.

Commercial organizations might prefer to limit the scope of actionable security breaches to those generating a "significant risk of identity theft or fraud". However, such a threshold is difficult to apply objectively, and if applied subjectively, leaves too much discretion in the hands of organizations with a vested interest in secrecy. Not surprisingly, it has generally been rejected in U.S. state laws.

Some organizations have raised the spectre of over-notification if the notification trigger is not limited by the presence of a "high risk" requirement. According to this theory, if the trigger for notification is too wide, individuals may become desensitized to the notices and will eventually ignore notices altogether. However, in various surveys, individuals have indicated that they wish to receive more information on security breaches and have the opportunity to take protective measures as they see fit.[6]

Moreover, the exercise of notification serves to document the problem that occurred and can help organizations mitigate the risk in the future. Finally, desensitization can be minimized by providing individuals with a risk assessment in the notification itself.

[6] 114 Ponemon Institute (26 September 2005) *National Survey on Data Security Breach Notification* at 3 and 9 and FTC/Synovate, *Identity Theft Survey Report* (Washington, D.C., September 2003) at 63.

Organizations should have the responsibility for determining whether or not the standard for data breach notification is met.

Generally, the affected organization is in the best position to calculate the associated risks of a breach of its information security and should be entrusted with this determination. However, there should be a requirement that every breach involving defined personal information be reported to the Privacy Commissioner, with full information about the nature and extent, the anticipated risks, mitigation measures, steps taken to notify affected individuals or, where notification is not considered warranted, the justification for not taking this step. (See below)

Who should be notified?

Notification of security breaches should be made to affected individuals, the owners of personal information, the Privacy Commissioner, government agencies, credit bureaus and law enforcement authorities. The Privacy Commissioner should be notified within five (5) business days of the security breach.

Affected individuals

Notice should be given to every person whose personal information has been compromised by the security breach. If it is not possible to identify individuals who have been affected by the breach, all those likely to be affected should be notified.

Organizations on behalf of whom the information was being held

If an organization maintains (the "maintainer") information on behalf of another organization, the maintainer should notify the other organization of the security breach. The other organization should have responsibility for notifying affected individuals and for indicating that the maintainer is the source of the breach. If two or more organizations are unable to come to an understanding as to which one has responsibility for notification, the organization that suffered the security breach should notify the affected individuals.

Privacy Commissioner

Notice of all security breaches should be made to the Privacy Commissioner within five business days of discovery of the breach, irrespective of whether the test for individual notification is met. Notifying the Privacy Commissioner ensures that a record is kept of all security breaches involving personal data, allows for oversight of organization practices, and offers the potential for organizations to obtain guidance from the Privacy Commissioner regarding notification obligations and methods.

Credit Bureaus

Canadian credit bureaus should be notified of security breaches as a matter of course, so they can monitor account activity and take steps to ensure that the privacy and credit rating of affected individuals are protected.

Government Agencies

Federal and provincial agencies, especially those that issue identification documents such as passports, Social Insurance Numbers and drivers licenses, should be notified of security breaches, as appropriate in the circumstances. The

Privacy Commissioner may give guidance to organizations as to which agencies should be notified in the context of a specific breach.

Law Enforcement Agencies

The Royal Canadian Mounted Police (RCMP) and other law enforcement authorities as appropriate should be notified of security breaches.

Form and Content of the Notice

Security breach notices should be separate from other communications and should include detailed information about the breach, including an assessment of the risk that the personal information of affected individuals will be used in an unauthorized manner.

Form of the Notice

To avoid any confusion, the notice should be a stand-alone communication. Notification should not be combined with another communication, such as account statements or marketing materials.

Contents of the Notice

Notices should include the following information:

- a general description of what occurred;
- the date and time of the breach (or the best possible estimate);
- the date and time the breach was discovered;
- the source of the breach (either the organization itself or the third party that maintained information on its behalf);
- a list of the type of personal information disclosed;
- an assessment of the risk of identity fraud as a result of the breach;
- a description of the measures taken or that will be taken to prevent further unauthorized access to personal information;
- contact information for affected individuals to obtain more information and assistance; and
- information and advice on what individuals can do to protect themselves against identity theft and fraud.

Risk Assessment

The risk assessment should include a simple rating of the risk such as "high", "medium" or "low". Organizations can further qualify this rating by providing more information.

Information on How to Protect Against ID Fraud

The legislation should prescribe specific minimum information that must be provided to individuals regarding what they can do to protect themselves from identity fraud arising from the breach.

Timing of the Notice

Security breach notification should be undertaken as soon as possible and without unreasonable delay after the occurrence of the breach, except where a law enforcement agency has made a written request for a delay. Delays for law

enforcement purposes should be for specified periods of time, and for no longer than 60 days at a time.

Any delay for law enforcement purposes should be permitted only where the RCMP or other law enforcement authorities have requested such delay in writing. Such delays should not exceed 60 days. The 60 day period could be extended if a delay is requested by the RCMP or other law enforcement authorities for investigative purposes.

Mode of notification

Notification should generally be by regular mail, but electronic and substitute notice should be permitted when certain conditions are met. Email notification should be permitted only if the individual concerned has consented explicitly to receiving important notices such as this by email. Substitute notice should be permitted where large numbers of individuals (e.g., 100,000) must be notified, where the total cost of individual notification is extraordinary (e.g., over $150,000), or where the Privacy Commissioner has specifically approved the substitute notice.

The cost of notification should be borne by the organization that incurred the security breach.

By Mail

Security breach notices should, as a matter of course, be sent by mail to affected individuals.

By Email

Consent to receiving marketing communications by email, for example, does not constitute consent to receiving important notices by email.

Substitute Notification

Possible substitute mechanisms include:

- telephone, fax or email;
- posting the notice conspicuously on the home page of the website and on login screens used by users to access their accounts on the company's website; and/or
- notifying major provincial media in each province where affected individuals reside.

Application to the Privacy Commissioner for substitute notice should include details on the proposed method of notice. The Privacy Commissioner should be empowered to require that a specific mechanism or a combination of mechanisms be used in order to ensure the efficacy of the notification.

Role of Privacy Commissioner

The Privacy Commissioner should keep records of all security breaches of which it receives notice, should provide guidance to organizations collectively and individually as appropriate, and should take an active role in raising public and

organizational awareness about security breaches. The Commissioner should also be empowered to order notification and substitute notice in appropriate cases.

Receive and Review Information about all Security Breaches

The Privacy Commissioner should be responsible for reviewing all reports of security breaches, and for ordering notification or substitute methods of notification where appropriate.

Compile statistics on security breaches

The collection of statistics by the Privacy Commissioner will assist in assessing the effectiveness of notification requirements and the progress of organizations over time.

Develop Expertise

By compiling statistics and by participating at various stages of the security breach notification process, the Privacy Commissioner will develop expertise in the area of security breaches. This expertise can be shared with organizations to help them in their efforts to combat security breaches.

Oversight

The Privacy Commissioner also has an important oversight function. The Privacy Commissioner should have the power to mandate that organizations take steps in order to prevent future security breaches.

Compel information disclosure

In order to accomplish its important role, the Privacy Commissioner should have the power to compel organizations to provide information on security breaches.

Penalties and Enforcement

Failure to notify individuals and organizations as required under the new law, as well as failure to comply with a Commissioner order under the law, should be treated as offences under PIPEDA and should be subject to meaningful and appropriate financial penalties.

There may be instances where an organization fails to notify individuals whose personal information is at risk as a result of a security breach. Some organizations may notify in an incomplete, ineffective or delayed manner. Tough penalties and enforcement thereof would help to ensure that organizations err on the side of disclosure and notification. For these reasons, there should be significant penalties for failure to notify where clearly required under the Act or where ordered by the Privacy Commissioner.

◆ ◆ ◆

This concludes the submissions of FIPA and BCCLA. We hope the Special Committee will find our suggestions useful, and in view of growing security problems and rising public

demands for privacy protection, will rise to the challenge of improving an already outstanding act.

BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION
#103 - 1093 West Broadway
Vancouver, BC V6H 1E2
Tel: (604) 739-9788 E-mail: fipa@vcn.bc.ca www.fipa.bc.ca