Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

CIPPIC Submission to Industry Canada re: PIPEDA reform issues

Response to Industry Canada's call for comments
in Canada Gazette, vol.141, no.43 (Oct.27, 2007)

January 15, 2008

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
57 Louis Pasteur, Ottawa, ON K1N 6N5
tel: 613-562-5800 x2553
fax: 613-562-5417
www.cippic.ca

Table of Contents

Introduction

1. By way of a public notice published in the Canada Gazette last fall, Industry Canada is seeking public input on a number of specific potential amendments to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), emanating from the Parliamentary review of PIPEDA held in 2006-2007. Industry Canada has requested input on the following specific issues/proposals:

   - the parameters of a data breach notification requirement
   - "work product" information: whether an amendment is needed
   - how to define "lawful authority"
   - witness statements
   - consent by minors
   - setting out PARTS elements in legislative form
   - alternatives to the current process for designating "investigative bodies"
   - any other issues related to the government's response to the *Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics on the PIPEDA.*

2. Below are CIPPIC's comments, focusing on three issues:

   - data breach notification
   - protecting the personal information of minors
   - PIPEDA compliance and enforcement

   Failure to address other issues does not reflect any particular position of CIPPIC on those issues. For reasons of limited time and resources, we are unable to address every issue of interest or concern.

3. CIPPIC is a legal clinic based at the University of Ottawa, Faculty of Law. Its mandate, in addition to student education, is to fill important voids in policy and law-making processes by representing under-represented interests on issues that arise as a result of new technologies. Upper year law students work under the supervision of the Clinic director and staff counsel on projects and cases involving the intersection of law, technology and the public interest. CIPPIC engages in policy development, legislative advocacy, public education, client advice, and precedent-setting litigation. Issues addressed include privacy, copyright, free speech,

domain name governance, and consumer e-commerce. Many clients come to the clinic for advice on privacy-related matters.

Data Breach Notification

4. In January 2007, CIPPIC published a White Paper entitled "Approaches to Security Breach Notification", in which we reviewed data breach notification requirements in the USA and Canada, and made specific recommendations for a similar requirement under PIPEDA.[1] Subsequently, the House of Commons Standing Committee on Access to Information, Privacy and Ethics recommended, in its May 2007 Report on PIPEDA, that PIPEDA be amended to include a data breach notification requirement. While differing with the Committee on the specifics of such requirement, the Government agreed in its Response that data breach notification should be legislated via PIPEDA.

5. As stated in the Gazette Notice, a statutory requirement for notification of data breaches "is 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."

6. Industry Canada has proposed that the new provision therefore include requirements (a) that the Privacy Commissioner be notified of any major breach of personal information, and (b) that affected individuals and organizations be notified when there is a high risk of significant harm resulting from the breach, and has requested further input on appropriate "thresholds" for when organizations should be required to notify.

6. CIPPIC agrees that there should be at least two distinct types of notification mandated by PIPEDA. Each type of notification should be subject to different rules and procedures according to on its purpose.

[1] CIPPIC's White Paper is accessible at <http://www.cippic.ca/identity-theft-2/> .

The Purposes of Data Breach Notification

7. As noted in the Gazette Notice, there are at least two distinct purposes of a data breach notification requirement:

   1) to "encourage organizations to implement more effective measures for the protection of personal information" ("security incentives"); and
   2) "enabling consumers to better protect themselves from identity theft when a breach does occur" ("individual mitigation").

8. A data breach notification requirement can, however, achieve additional valuable purposes if constructed appropriately. These include:

   3) to provide the basis for more effective and targeted compliance actions ("compliance measures") through the ability to monitor the frequency, nature and trends of data breaches and to identify persistent or systemic problems at an early stage;
   4) to inform future policy-making through the creation of a database of information about security breaches that is available to r policy analysts ("policy analysis"); and
   5) to improve the functioning of a competitive marketplace through greater consumer awareness of risks both general and company-specific ("marketplace information").

9. The Government's preliminary proposal is for two separate notifications: (a) to the Privacy Commissioner ("OPC") and (b) to affected individuals. We agree that both the OPC and individuals should be notified, as each serves a different set of policy goals.

10. Notifying the OPC provides the basis for:

    a) effective and targeted **compliance measures** (including assisting organizations in identifying cases in which individual notification is appropriate); and
    b) internal government **policy analysis** based on a solid factual foundation.

11. Notifying affected individuals achieves the purpose of allowing those individuals to **mitigate** the risk of identity theft/fraud created by the breach. It also has two valuable side-effects in terms of **security incentives** and **marketplace information**:

    i) by creating the risk of bad publicity, it goes some distance toward creating incentives for businesses to take effective security measures that prevent data breaches in the first place; and

ii) to the extent that consumers generally become more aware of risks both general and company-specific, improving the functioning of a competitive marketplace.

12. Three of the five policy goals mentioned above (security incentives, policy analysis, and marketplace information) are however not fully achieved under this approach. In particular, security incentives are dependent on leakage of individual notices to the media rather than direct notice; policy analysis is limited to those who have access to the non-public information provided to the OPC; and only a limited amount of marketplace information is made available to a limited number of consumers.

13. A national, publicly available, electronic registry of data breaches, in addition to OPC and individual notification, would, if constructed appropriately, achieve the goals of security incentives, marketplace information, and policy analysis much more effectively than would OPC and individual notifications on their own.

A Centralized Data Breach Registry

14. Incentives for strong security are created when companies perceive a significant risk of widespread negative publicity in the event of a breach.[2] Individual notification requirements create the possibility of such publicity, but in an inefficient, indirect way: the media are not necessarily informed. Indeed, the cases that reach the media via individuals may not be those most deserving of media attention.

15. A more efficient and effective way to achieve the goal of incentive creation is to establish a public database of all data breaches accessible to the public. This way, journalists have a much better basis on which to decide which breaches are newsworthy and which are not, and companies face a much higher risk of bad publicity in the event of a significant breach.

16. Moreover, researchers outside the government would have access to the public registry and could conduct valuable policy analysis based on it. The public would benefit not only in a broad sense from such distributed research and analysis, but also, as consumers, in a very direct sense from access to relevant marketplace information. Public policy would be

[2] *Security Breach Notification Laws: Views from Chief Security Officers* (Samuelson Clinic, University of California-Berkeley School of Law, Dec.2007).

improved as a result of open access to a comprehensive set of accurate information about data breaches in Canada, and the marketplace would function more effectively as a result of better informed consumers.

17. CIPPIC therefore strongly recommends the establishment of a centralized, public registry for tracking data breaches in Canada. Organizations should be required to report to the registry all security breaches involving the exposure of personal data to unauthorized access.[3]

18. Consideration may be given to limiting "personal data" for the purposes of this rule to designated information, as is currently done in a number of U.S. statutes.[4] Under such an approach, it is important to ensure that the designated information includes all information that could put an individual at risk of identity fraud.

19. The threshold for public registry reporting should be relatively low, given that the registry will include sufficient information (see next paragraph) to distinguish major breaches from minor breaches. A low threshold is also appropriate given the policy analysis and marketplace information purposes of the registry: the more information available (in a form conducive to analysis), the more useful it will be for researchers and consumers. Finally, the costs to organizations of reporting to the registry will be minimal, since they should have gone through an internal analysis generating this information in any case, and therefore need only report it.

20. Reports to the registry should include key information needed (a) by the media, to distinguish between significant and insignificant breaches, (b) by consumers, to make informed purchasing decisions, and (c) by researchers, to analyse relevant trends and issues. Such information should include:

    a) company name, sector, size, title and contact information for responsible official,
    b) type of data compromised,
    c) type and number of accounts compromised,
    d) number of individuals affected,

[3] Exceptions may be specified – e.g., for cases in which access was limited to employees of the organization, where such employees are bound by confidentiality rules protecting the data in question.
[4] See CIPPIC White Paper, pp.24-25.

e) source of data compromised (direct from consumer, other sources),

f) nature/cause of breach, if/once known (e.g., stolen laptop, unintended online exposure, external hack of database, loss of tape/hard drive, unauthorized access to server, etc.), and

g) date discovered, period of time affected, date reported.

21. The registry can and should be constructed in such a way that companies post information directly to it, that reporting is standardized, and that the information is stored and displayed in a manner conducive to easy review and analysis. Once established, the registry should require little effort to administer.

22. Public disclosure of certain information about the breach may create additional risks for affected individuals. In such cases, the information in question should be withheld initially and posted as soon as the risk of its abuse has disappeared (e.g., after the breach has been resolved and individuals have been notified).

23. Note that the creation of a centralized, publicly-available registry of data breaches does not replace the need for individual and OPC notification, but instead is complementary to them. As noted above, it improves significantly upon the proposed combination of individual notification and non-public reporting to the OPC by:

a) giving the media a single, comprehensive, and reliable source of information about data breaches from which they can make more informed decisions about what to report on;

b) giving researchers other than those with access to the OPC database the opportunity to review and analyse trends over time, with a view to improving our understanding of the issue so as to develop more effective strategies for addressing it; and

c) allowing <u>all</u> consumers, not just those affected, to inform themselves (or to be informed by consumer advocates) of relevant marketplace risks.

Reporting to the Privacy Commissioner ("OPC")

24. Regardless of other reporting requirements, organizations should be required to report breaches to the OPC given that this office is responsible for administering the relevant law. Even if the OPC has no duty to determine whether notification is required in a given case, it may be in a position to assist organizations struggling with their legal obligations. Moreover,

as the administrative body overseeing PIPEDA, the OPC should have at its disposal as much information as possible regarding compliance.

25. The threshold for notifying the Privacy Commissioner of breaches involving personal information should be designed to capture all breaches of interest from a policy and law enforcement perspective. In our view, this includes all breaches in which personal data was exposed to unauthorized access (the same standard we propose for reporting to the public registry).

26. The proposed threshold of "major loss or theft of personal information"[5] sets a standard which is both unclear and unnecessarily high. First, whether or not a given loss of personal information is "major" will undoubtedly be a subject of debate. Much greater clarity is needed in order for organizations to be able to judge whether or not notification is required.

27. Second, "major loss" sets too high a standard for this notification. It excludes not only "minor" losses but also everything in-between: i.e., all breaches that, although more than minor, are not major. At a minimum, all but minor breaches should be reported. Nevertheless, as noted above, there is value in notifying the OPC of even minor breaches. It allows for regulatory oversight of organizations' determinations, and provides the OPC with valuable information for ongoing and future policy analysis.

28. Because it involves no risk of publicity, and because the Office of the Privacy Commissioner may be able to assist the organization in determining the appropriate steps to take to mitigate the effects of the breach, this notification should be made without delay, as soon as the organization becomes aware of the breach.

29. Such notification should contain prescribed information and be in a prescribed form such that it can be automatically added to the OPC's database for future reference and analysis. Reports to the OPC should include at least the same information required by the public registry (see above). Additional information should include the circumstances of the breach, foreseeable harm from the breach, and steps taken to notify individuals (or justification for not doing so). Information too sensitive to include in the public registry should be reported to

[5] Government Response, Recommendation 23.

the OPC. Initial reports should be made without delay, and additional information provided as it becomes available.

Reporting to Credit Bureaus

30. In case of breaches involving personal financial information, or where there is a foreseeable risk of financial identity fraud, credit bureaus should be notified so that they can flag the relevant accounts. However, it is important that affected individuals not be unduly inconvenienced as a result of the resultant fraud alerts; provincial consumer reporting laws should be reviewed to ensure that they offer sufficient protection to consumers from undesirable effects of fraud alerts placed on their files.

31. The government has requested input on, among other things, the need for a "without consent" power to notify credit bureaus of data breaches. Subs.7(3)(i) of PIPEDA allows for disclosure without knowledge or consent where "required by law". If organizations are required by PIPEDA to disclose to credit bureaus the identity of breach victims, this would, in our view, satisfy the subs.7(3)(i) requirement.

Individual Notification

32. The goal of giving individuals the information they need to mitigate potential harm from a given breach can be achieved only by notifying individuals directly. Thus, individual notification should be required in any case. As noted above, individual notification also serves the goals of creating stronger security incentives and providing marketplace information, but does so less effectively than would a centralized, public registry.

33. Given its primary purpose, the threshold for notifying individuals should be designed to capture <u>all breaches that generate a risk that the individual's personal information will be used in contravention of PIPEDA.</u> Individuals deserve to be notified when they are put at risk by the actions (or omissions) of another party.

34. A risk-based standard reduces the need to specify types of data covered and/or exempted data, as such facts (e.g., whether or not the data was encrypted) will go into the determination of whether or not the risk threshold is met.

35. We prefer a "misuse" rather than "harm"-based standard for two reasons: first, individual privacy is valuable and deserving of protection *per se* even where its breach does not lead to measurable harm. This is the fundamental premise on which PIPEDA is based; harm may be necessary to prove in order to obtain damages, but it is not an essential element of informational privacy breaches.

36. Second, harm caused by privacy breaches tends to be cumulative: although the initial breach may entail no obvious immediate risk of harm to the individual, the cumulative impact of information gathering, analysis and sharing (including information gathered via a breach) can lead to significant harm over time. Identity thieves, for example, may gather information about an individual over time, from a variety of sources, until they have sufficient data to impersonate their victim and fraudulently acquire loans in the victim's name. An approach that looks only at immediate harm will not capture these serious risks.

37. The Government has proposed a standard for individual notification of "*high* risk of *significant* harm to individuals or organizations" (emphasis added). This is an extremely high standard, requiring notification only in those cases where (a) the potential harm caused by the breach is "significant", and (b) where the risk of such harm is "high". As the Table below shows, this threshold excludes not only cases where there is a low risk of harm or where the potential harm is insignificant; it also excludes those cases in which there is a high risk of moderate harm (i.e., less than significant but more than insignificant), and those where there is a moderate risk of significant harm.

	Significant Harm	Moderate Harm	Insignificant Harm
High Risk			
Moderate Risk			
Low Risk			

38. If a "gradation of risk and harm" approach is taken, all but low risk and/or insignificant harm cases should be subject to the notification rule. Individuals deserve to be notified, at a minimum, in all cases other than those where the risk of harm is low, or where the potential

harm caused is insignificant. Indeed, CIPPIC submits that individuals deserve to be notified in all cases where the potential harm caused is more than insignificant, even where the risk is low. The rule should therefore require notification in all cases where there is a risk of harm to individuals or organizations, except where the potential harm is insignificant.

39. In any event, and especially if the standard adopted involves an assessment of risk and/or of the significance of harm potentially caused, organizations will need guidance as to what types of risks meet or do not meet the threshold. **CIPPIC therefore recommends that a regulation be adopted setting out, for greater certainty, specific factual circumstances that meet (or do not meet) the test.** For example, it could be stated that financial loss, adverse credit effects, or personal embarrassment, all constitute "significant harm". We recommend that a working group with multi-stakeholder representation be constituted to assist Industry Canada with the development of such a regulation.

40. Needless to say, the test must be objective: a legal requirement that leaves it up to organizations to decision whether or not the criteria for notification is met in any given case and that does not provide for oversight and challenging of that determination, is pointless. Organizations will have to make the determination in each case, but they must be held to an objective standard, and their determinations must be reviewable. Failure to notify in cases where the objective standard is met should result in meaningful penalties (see below).

41. Notices to individuals should contain prescribed information designed to assist individuals in mitigating the risk in question. In addition to information about the breach, its timing, the personal data involved, and what the organization has done to mitigate the risk, the notification should include what the organization will do to assist individuals, what the individual can do to protect him or herself, and contact information for the organization as well as other relevant agencies. The OPC Guidelines for Organizations in Responding to Privacy Breaches[6] address this issue well.

42. In order to avoid any confusion on the part of consumers, it is essential that the notification be a stand-alone communication, separate from marketing and regular account statements. It

[6] See http://www.privcom.gc.ca/information/guide/index_e.asp. Note that these Guidelines were developed by industry representatives together with the OPC.

should not in any way be associated with marketing or promotion by the organization. As the OPC Guidelines note, direct notification is always preferred, and indirect notification (e.g., via the organization's website, in mainstream media announcements) should only be used in exceptional cases where direct notification could cause further harm, is prohibitive in cost, or where individual contact information is not known.

43. Email notification should be considered sufficient only if the individual in question has explicitly consented to receiving important information from the organization by email at that particular email address. This is important because of the tendency for organizations to use email primarily for marketing (as opposed to contractual) purposes. Important messages from the organization may therefore be caught by spam filters or simply lost in the flood of spam received by consumers.

44. CIPPIC continues to recommend, as it did in its Jan.2007 White Paper, that individual notification 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.

45. It should be noted that the appropriate threshold for and content of individual notification may vary according to whether or not a public registry is established, and what information is made available through the registry. To the extent that the public registry fulfils the policy goal of improving security incentives, individual notification need not be designed for that purpose. If individual notification, on the other hand, is meant to create general security incentives as well as to help individuals mitigate harm, the threshold for notification should be higher. Similarly, to the extent that the registry provides marketplace information to consumers generally, the content of individual notification can be focused on individual harm mitigation.

46. Finally, those resisting a relatively low threshold for individual notification frequently make unsupported assertions about "notice fatigue" by consumers. This is a specious argument on two counts. First, it lacks an evidentiary basis. Second, even if evidence is found to support

the assertion, the argument fails on the grounds that individuals who read and appreciate the notice should not be denied it simply because others disregard it.

Penalties for Failure to Notify

47. If a breach notification requirement is to be effective, it must be backed up with meaningful penalties via either state enforcement or private action. PIPEDA's current enforcement regime is extremely weak, resulting in widespread non-compliance with even basic requirements.[7] There is no reason to believe that compliance with a new breach notification requirement would be any different, if treated like most other obligations under PIPEDA. Something more than non-binding Privacy Commissioner findings and subsequent recourse to Federal Court is needed if a breach notification requirement is to be effective.

48. Currently, PIPEDA treats as offences, subject to state prosecution and fines, only the following:

    a) destruction of data already subject to an access request;
    b) disciplining an employee for good faith disclosures, refusals or other acts regarding compliance with PIPEDA;
    c) obstructing the Commissioner in an investigation or audit.

49. To this list should be added failure to disclose a known data breach as required by the new provision. In keeping with the current approach to offences, which focuses on bad faith acts or omissions in violation of unequivocal legal requirements, the offence could be limited to failures to notify in cases where the obligation is clear (as opposed to cases where it is debatable whether or not the threshold has been met).

50. Even if failure to notify is made an offence under PIPEDA, the enforcement of new breach notification requirements should not be left entirely to the state. Individuals, and the Privacy Commissioner, should be empowered to call organizations to account legally for failure to notify. The most effective way of doing so is via private class actions, with associated statutory damages. PIPEDA should be amended, in any case, to permit class actions (see below, under "PIPEDA Compliance and Enforcement").

[7] See CIPPIC, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (April 2006).

Children's Privacy (Personal Information of Minors)

51. In its response, the government has expressed support for the Committee's recommendation that amendments be considered to deal with the special problem of children's informational privacy, and has asked for submissions on this topic.

52. In its Nov.2006 submission to Parliament, CIPPIC recommended that PIPEDA be amended to include "specific rules limiting the collection, use and disclosure of children's personal information. Such rules should be at least as strict as those already adopted in the *Canadian Code of Practice for Consumer Protection in Electronic Commerce* and by the Canadian Marketing Association. There should be strict and significant penalties for violating these provisions."

53. PIPEDA does not currently apply any special rules to the collection, use and disclosure of personal information of children. Instead, it sets out general rules and principles - including consent requirements and "appropriateness" criteria - that must be interpreted and applied to each fact situation. Interestingly, and despite the development of a whole industry of child-centered commercial websites, there appears to have been very little interpretation of these rules as they apply to the collection and use of information about children.

54. The Canadian Marketing Association Code of Ethics[8] sets out rules requiring express consent, either from parents or from the child, depending on the child's age and the type of information, for the collection, use or disclosure of personal information for marketing purposes. While these rules (applicable to CMA members only) are certainly an improvement on PIPEDA's silence as to what is appropriate, and therefore permissible, in terms of the collection, use and disclosure of children's personal information, they do not go far enough in CIPPIC's view.

55. Subs.5(3) of PIPEDA states:

> An organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

[8] See http://www.the-cma.org/?WCE=C=47|K=225849#11 .

56. CIPPIC submits that reasonable people would consider it inappropriate for organizations to collect, use or disclose personal information about children for marketing or other secondary purposes, period. While the appropriate age threshold for such a rule is debatable, it should at a minimum apply to children under the age of 13.

57. Consent in such cases should be a non-issue in the context of children's privacy because it is so fraught with problems. Clearly, children have not developed the knowledge and experience required to give properly informed consent themselves – that is why the CMA, as well as U.S. legislation,[9] requires parental consent for the collection, use or disclosure of personal information from children under 13 years of age ("verifiable parental consent" in the case of the U.S. legislation). But even parental consent requirements are of limited effectiveness insofar as they are easily circumvented by children, who can impersonate their parents or simply lie about their age to avoid the parental consent requirement in the first place. Moreover, parents themselves may not appreciate what they are being asked to consent to on behalf of their children, given how long, unclear and incomplete privacy policies typically are.[10]

58. As Professor Valerie Steeves has pointed out,

> "…the online invasion of privacy is not merely a question of collecting personal information from children without their, or their parent's, consent. Rather, it involves the opening up of the child's private world to the eye of the marketer, who not only watches the child but reconstructs the child's environment in order to manipulate the child's sense of self and security."[11]

59. Instead of relying on relatively ineffective consent-based rules, the protection of children's privacy should be based on clearly delineated limits to information collection, use and disclosure. In CIPPIC's view, this is precisely what subs.5(3) of PIPEDA is designed to accomplish. However, its general language needs to be supplemented with specific

[9] *Children's Online Privacy Protection Act of 1998* ("COPPA"), 15 U.S.C. 6501-6506.
[10] CIPPIC, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (April 2006).
[11] "It's not Child's Play: The Online Invasion of Children's Privacy", *University of Ottawa Law and Technology Journal* vol.3, no.1 (2006), 171-188 at 186. See also Burkell, Steeves and Micheti, *Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand* (2007), http://idtrail.org/content/view/684/42/ .

provisions addressing the collection, use, retention and disclosure of children's personal information, so as to provide greater certainty and guidance to organizations.

60. In particular, we propose a new provision (e.g., subs.5 (3.1)) setting out rules such as the following:

> *For greater certainty, the following purposes would be considered by a reasonable person to be inappropriate in the circumstances:*
>
> *(1) targeted marketing, with respect to children under the age of 16;*
>
> *(2) any purpose other than those reasonably understood by the child or parent at the time and in the context in which the information was originally collected, with respect to children under the age of 18;*
>
> *(3) any purpose, with respect to the retention, use or disclosure of personal information about children once they reach the age of 18.*

61. In other words, PIPEDA should clearly and simply prohibit the collection, use, and disclosure of personal information about children under the age of 16 for target marketing purposes. It should also prohibit the collection, use and disclosure of personal information about children under the age of 18 for any purpose other than those reasonably understood by the child or parent at the time that the information was originally collected. These rules should apply regardless of purported "consent".

62. In addition, PIPEDA should require that organizations holding information about children destroy that information once the child reaches the age of 18. This requirement acknowledges that children typically act in ways that could prejudice or embarrass them later in life, and is designed to allow adults to redeem themselves in the context of an electronic world that records everything we do and say.

PIPEDA Compliance and Enforcement

63. The Government has invited submissions on any issues related to the government response to the Standing Committee's Report on PIPEDA. CIPPIC would like to comment on the issue of PIPEDA compliance and enforcement.

64. As noted in its November 2006 submission, CIPPIC considers PIPEDA's woefully inadequate redress and enforcement regime to be the single most important issue for consideration in the PIPEDA review. Unfortunately, this issue did not receive the attention it deserved by the Committee. Instead, the Committee simply accepted the unsupported assertion, repeated by a string of self-interested business representatives and public officials, that PIPEDA is working well and is not in need of significant structural change. This view, reflected in the government response, flies in the face of the evidence.

65. A rigorous study conducted by CIPPIC in 2006 indicates widespread non-compliance with the PIPEDA.[12] The study, the first ever significant survey of business compliance with the Act, focused on retailer compliance with four basic requirements of PIPEDA: openness, accountability, individual access, and consent. A total of 64 retailers were assessed (72 in the case of individual access). In short, the results indicated widespread non-compliance in all four areas, by large as well as small organizations.

66. Others have noted that under the current regime, "regulated parties are able to ignore the Comissioner's decisions with impunity",[13] "[business] implementation of the PIPED Act has been *ad hoc* at best and non-existent at worst",[14] companies found in violation of the Act remain non-compliant,[15] and "for many organizations privacy compliance has ceased to be a serious legal obligation. Instead, for many it is considered a business risk that carries no

[12] *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (CIPPIC, May 2006).
[13] BCCLA, *Securing Compliance, Protecting Privacy: The PIPEDA Enforcement Evaluation Project* (March 2006), p.83.
[14] "*Implementing PIPEDA: A review of internet privacy statements and on-line practices",* University of Toronto Centre for Innovation Law and Policy (May 6, 2005), quote from Executive Summary; <http://pipedaproject.rcat.utoronto.ca/>
[15] John Lawford, *Consumer Privacy under PIPEDA: How are we doing?* (PIAC: Nov.2004), pp.44-55.

realistic expectation of serious financial consequences or diminished reputation — a risk that can be managed through minimal compliance and contrition if caught".[16]

67. Based on the known facts, which have not be contradicted, there can be little dispute that the current model is insufficiently effective and that change is needed.

68. In its submissions to the Parliamentary Committee, CIPPIC proposed a number of amendments designed to improve industry compliance with the Act. These included:

- Commissioner use of the subs.20(2) power of publicity to "name and shame" organizations who fail to comply with the Act;
- greater Commissioner use of audit powers both for random "spot checks" and for more in-depth audits of organizations against whom complaints have been made;
- providing the Commissioner with order-making powers (as is the case in all three provinces with similar data protection laws);
- establishing a new Tribunal with order-making powers, to which complainants and/or the Commissioner can take unresolved complaints and obtain damages;
- providing individuals and classes of individuals with a statutory right of action through which they can hold organizations accountable and obtain damages;
- allowing organizations (e.g., CIPPIC) and groups of individuals to lodge complaints and obtain injunctive relief on behalf of others;
- allowing for punitive as well as compensatory damages; and
- treating willful contraventions of the Act and/or failure to comply with Commissioner orders as offences, subject to financial penalties.

69. CIPPIC noted in its submissions that these options are not mutually exclusive, and that a combination of approaches is likely to be most effective.

70. Yet, the Committee (and hence, the government in its response) addressed only two of these proposals: giving the Commissioner order-making powers, and making Commissioner use of the subs.20(2) “naming” power mandatory in cases of non-compliance (Recommendations 18 and 19 of the Committee Report). Both were rejected by the Committee, and subsequently by the government.

[16] "Rising to the Privacy Reform Challenge", *Toronto Star* (Oct.25, 2004).

71. None of CIPPIC's remaining six proposals for more effective compliance incentives and enforcement of the Act were even acknowledged by the Committee or the government. Yet they offer low cost and potentially effective means of improving compliance with the Act. In particular, CIPPIC urges the government to give serious consideration to the following proposed amendments designed to improve compliance with the Act:

    a) provide individuals and classes of individuals with a statutory right of action through which they can hold organizations accountable and obtain damages; alternatively, amend s.14 to permit class actions, including applications by similarly affected individuals who have not lodged complaints under s.11;
    b) protect *bona fide* applicants under s.14 of the Act (or for judicial review of PIPEDA decisions) from adverse cost awards in Federal Court, and provide for solicitor-client costs in the event of successful applications;
    c) amend s.16 of the Act to provide for punitive as well as compensatory damages, and possibly for statutory damages in certain circumstances.

72. We look forward to ongoing consultations with Industry Canada and other stakeholders in the effort to craft workable amendments designed to make PIPEDA more effective.

Yours truly,

Original signed

Philippa Lawson
Director, CIPPIC