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

Philippa Lawson
Director
(613) 562-5800 x2556
plawson@uottawa.ca

28 April 2008

Richard Simpson
Director-General,
Electronic Commerce Branch, Industry Canada
300 Slater Street
Ottawa, Ontario K1A 0C8

BY EMAIL and MAIL

Dear Mr. Simpson,

Re: PIPEDA Review – Data Breach Notification: Proposed Model

We are writing to provide comments on the Proposed Model for Data Breach Notification issued by your office by way of a document dated March 27, 2008, and discussed at a stakeholder meeting on April 11, 2008. I regret that CIPPIC was unable to participate in that meeting other than by way of observation by our articling student, Jocelyn Cleary. We do however appreciate this opportunity to comment on the matters discussed at that meeting.

Scope

The proposal is to amend PIPEDA so as to provide for an explicit data breach notification requirement. While this makes sense for the private sector, we wonder why a similar provision is not being considered for the public sector. Individuals deserve to be notified of data breaches exposing them to potential ID fraud regardless of the source of the data breach.

The House of Commons Standing Committee on Access to Information, Privacy and Ethics is currently undertaking a review of the *Privacy Act* with a view to potential amendments. Is there a reason why Industry Canada is not proposing that the *Privacy Act* be amended to include a data breach notification requirement?

Legislative Framework

The Act should contain a general requirement for notification and reporting, along with criteria for such notification and reporting where such criteria are meant to be enduring. Matters that are more susceptible to change over time should be left to regulation. Such matters include more specific criteria for notification/reporting, including concrete examples, and rules regarding the timing and format of notices.

Definition of Data Breach

We concur with Industry Canada's proposed definition of "data breach", focusing on disclosure, loss and third party access – i.e., "an incident involving unauthorized disclosure of, loss of, or access to personal information". We oppose any further narrowing of this definition (e.g., requiring that the disclosure/loss/etc. be "unintended" as well as "unauthorized", or that the information in question is susceptible to misuse or harm). Risk of harm is relevant to the threshold issue of whether or not to report/notify, not to whether the data breach constitutes a data breach in the first place. Intentions of the organization suffering the data breach should be irrelevant.

The tests for notification and reporting: objective vs. subjective

It is our understanding that organizations will be held to an objective standard for both reporting breaches to the Commissioner and notifying affected individuals. In other words, while organizations are responsible for making the call as to whether the breach meets the legal requirements for reporting and notifying, they may be held liable for making the wrong call. The subjective views of the organization are irrelevant; the standard is an objective one, subject to review after the fact if the organization's determination is challenged.

It makes no sense for the test to be subjective – the law would then have no substance; there would be no way to enforce reporting. Organizations currently report breaches and notify individuals when they consider appropriate. The only reason to introduce a law requiring notification and reporting is to force organizations to notify and/or report when they would otherwise not do so.

We are concerned that the Proposed Model does not make this clear, and that some parties may persist in the misunderstanding that organizations will not be held to an objective test for reporting and notifying individuals of data breaches. For example, section 7(b) proposes that notification of data breaches be required "where *it is determined that* there is a high risk…." This suggests that the test is subjective – that as long as the organization determines that there is a less-than-high risk, they need not report (even if the risk is in fact high). This matter needs to be clarified. Section 7(a) of the discussion paper should specify that although organizations are responsible for determining whether notification is required, they will be held to an objective standard for such determination. Similarly, section 8 of the discussion paper should specify that the standard for reporting is objective.

Threshold for notifying individuals

The proposed threshold for notifying individuals of breaches involving their personal data is "high risk of significant harm". As noted in our January 15th submission to

Industry Canada on PIPEDA Reform, this standard is much too high, leaving out cases in which there is a reasonable but less than "high" risk of significant harm to the individual, and in which there is a high risk of moderate but not "significant" harm. We propose an inverse approach to the standard, in which all breaches are reported *other than* those involving a low risk of harm to the individual. Individuals deserve to be notified when organizations fail to protect their data from unauthorized access as long as there is any reasonable risk of consequent harm to them.

The wording of this standard is critical in our view, even if criteria are developed to assist organizations in applying the test to specific situations. The terms "high" and "significant" have meaning, and will mean the difference between reporting and not reporting in many cases.

The discussion paper defends the proposed approach by noting that "if experience shows that the threshold has been set too high, [it] can be adjusted". But experience is unlikely to show this, as long as the public is unaware of many breaches, and as long as all breaches need not be reported to the Privacy Commissioner. Experience is more likely to be an effective guide if we start with a higher standard.

Criteria for "[high] risk of [significant] harm"

The paper refers to criteria for notification, but does not propose any. Instead, it merely lists a number of factors to be considered. Factors are helpful, but are not the same as criteria. We agree that criteria are needed so as to make the test clearer and easier for organizations to apply in given fact situations. Each factor listed in the paper should be translated into a criterion. For example, "sensitivity of information involved" could become "information that is vulnerable to fraudulent use or that could be used by a third party to embarrass, prejudice, or otherwise harm the individual".

In order to make the objective test as easy as possible to apply, specific examples should also be provided. In particular, particular types of information that are sensitive (e.g., credit data, account numbers, social insurance numbers) and thus loss of which should always trigger notification should be specified.

It is important to note that criteria, like factors, need not - indeed, should not - be exhaustive.

We are willing to work with Industry Canada and other stakeholders to identify specific and general criteria for notification.

Threshold for reporting to the Privacy Commissioner

The new proposal is for organizations to report all "material breaches" to the Privacy Commissioner. We agree that this is a more appropriate threshold than "major loss or

theft of personal information". However, the term "material" is unnecessarily vague: if what is meant is "non-trivial", then why not say so? For purposes of clarity, we suggest the term "non-trivial" rather than "material". It is important that the Privacy Commissioner receive notice of all non-trivial (or "material") breaches in part so that she can monitor the situation and identify cases in which notification should have, but did not, occur.

Criteria for "material breach"

Once again, the proposal sets out a number of factors to consider in deciding whether or not a given breach is "material", but does not propose any criteria. As for notification to individuals, the general test for reporting to the Commissioner should be supplemented by criteria that are as specific as possible. Such criteria need not be exhaustive; their purpose is to make the objective test as easy as possible to apply in any given fact situation. It may be easier to specify criteria for <u>not</u> reporting – i.e., to require reporting of all breaches except those that are trivial, and to establish criteria for triviality.

Timing of reporting to the OPC

The proposal would require organizations to report breaches to the OPC "within a reasonable period of time after detection of the breach". This leaves wide open the determination of what constitutes a "reasonable period". Especially since there is no risk of publicity as a result of this reporting, we submit that a period of time such as 14 days should be specified, along with the requirement for an explanation if more time is taken.

Availability to public of reports on Data Breaches

The proposal is for information on data breaches to be compiled and made publicly available in aggregate form by the OPC, at her discretion. In our view, compilation and publication of such information should be a <u>duty</u> of the OPC; it should not be left to her discretion. This is particularly important if our proposal for a public registry of data breaches (see below) is not adopted, or if the public cannot access data breach reports via formal Access to Information requests.

Some parties apparently objected to the public accessibility via Access to Information requests of their reports to the OPC, presumably out of concerns that the reports may contain information that could be useful to criminals seeking to take advantage of data breaches. Such concerns are unwarranted, insofar as the *Access to Information Act* already provides exemptions for such purposes. Section 16(2) of the Act, for example, states:

> "The head of a government institution may refuse to disclose any record requested under this Act that contains information that could reasonably be expected to

facilitate the commission of an offence, including, without restricting the generality of the foregoing, any such information
(*a*) on criminal methods or techniques;
(*b*) that is technical information relating to weapons or potential weapons; or
(*c*) on the vulnerability of particular buildings or other structures or systems, including computer or communication systems, or methods employed to protect such buildings or other structures or systems."

Publication of Data Breach Incidents

In our submission to Industry Canada on the PIPEDA Review, dated January 15, 2008, CIPPIC called for a public registry of data breach incidents. This proposal is not mentioned in the Industry Canada discussion paper, and was apparently not discussed at the meeting. We believe that it merits consideration, for the reasons set out in our January submission.

In particular, a public registry would have the benefits of:

a) creating a more effective incentive effect for stronger security measures by organizations than would be accomplished by individual notification alone;
b) allowing the media, consumers and policy-makers to see the full picture and thus to make more informed decisions;
c) over time, creating a useful database of information upon which more informed policy-making can be based.

We understand that industry stakeholders have expressed concerns that making such information public could (a) compromise security, and (b) provide fodder for class actions against them. With respect to security concerns, our proposal is not to require the reporting of information that could be used by criminals to engage in additional fraud. Indeed, we explicitly acknowledge the need to identify types of information that can be reported without risk of abuse, and to limit reporting obligations to that information. With respect to the industry fear of class actions, we respectfully submit that organizations should be held accountable for their negligence, and that class action processes are carefully designed so as to permit only those with merit to proceed.

We therefore urge the government to consider our proposal for a public registry.

Yours truly,

Original signed

Philippa Lawson