

Speaking Notes

**Philippa Lawson, Executive Director & General Counsel,
Canadian Internet Policy and Public Interest Clinic (CIPPIC)**

to the

**House of Commons Standing Committee on Access to Information, Privacy and Ethics
in re: the first statutory five year review of the
*Personal Information Protection and Electronic Documents Act ("PIPEDA")***

December 6, 2006

Thank you for the opportunity to testify before you today.

In the few minutes I have, I'd like to go over some of the key findings of CIPPIC's two recent studies, which were mailed to each of you last week. I'll then highlight PIPEDA's major flaws and suggest ways of correcting them.

For more specifics, I refer to you our written submission dated November 28th. That submission includes a brief description of CIPPIC and of my background, as well as a detailed list and explanation of our 20 recommendations.

I have been working in the privacy field for about 15 years, primarily as a consumer advocate. Since the early 90's, I have worked closely and productively with the Canadian Marketing Association, the Retail Council of Canada, the Bankers' Association, ITAC, telecom companies, and other business interests on various privacy-related matters, including the Code that forms the basis of PIPEDA.

Since starting up CIPPIC in 2003, my focus has been to make privacy laws work by researching marketplace practices, exposing questionable practices, and holding organizations accountable.

I have been a staunch advocate of PIPEDA since its conception and I continue to be a strong supporter of the Act. However, with almost six years of experience with PIPEDA under our belts, it has become clear that there are a number of gaps and flaws in the regime.

I'd like to talk first about what we found when we researched the Canadian data brokerage industry.

We found many instances of consumer lists for sale or rent, where the likelihood that those consumers had truly consented to the subsequent trading of their names and contact information was highly questionable.

For example, one list we found has information about individual and household lifestyles, hobbies and demographics on almost 900,000 Canadians. The information comes from "product registration cards" filled out by consumers.

Another list has the age, gender, home address, and telephone numbers of almost 50,000 "Frequent Travellers in Canada". The information was obtained from corporate client databases of airline ticketing offices and travel agencies.

Another list has the gender, monthly income, home and business address of almost 13,000 Canadians with Gold Cards. The information came from "payment processing companies".

We found numerous lists offering detailed health information about Canadians, who had provided the information on websites or in response to surveys.

I could go on and on. The point is: there is a vibrant industry in the compilation and trading of these lists, for direct marketing and potentially other purposes. And it is not at all clear that individuals on these lists have consented to such use of their information.

The second study we did, called "Compliance with Data Protection Laws", was conceived and designed for the very purpose of this review. We tested the compliance of 64 online retailers with three of PIPEDA's most basic requirements: openness, accountability, and consent.

Our sample included large and small companies, and covered nine different types of business from magazines to general retailers. We also tested the compliance of a separate sample of 72 companies with PIPEDA's requirement for individual access.

The results were sobering. In brief, we found widespread non-compliance with the Act.

Over half of the 64 companies we contacted by phone could not provide contact information for the person in the company responsible for privacy. Two thirds refused to provide their privacy policy by any means other than their website.

Looking at privacy policies, 70% were incomplete in some important respect. 22% were unclear about why they collect the information, 30% were unclear about how they use the information, and 45% were unclear about to whom they disclose the information.

A third of companies we tested don't bother to get consent during the online ordering process. Most companies rely on their privacy policies to get consent, but over half fail to bring the policy to the attention of shoppers, and 60% bury the opt-out inconspicuously in the policy.

We found a disturbing number of misleading representations in the policies or on the websites, suggesting for example that the company would not share your information without consent, but then, deep down in the policy, stating that your consent was being assumed.

Somewhere between 11% and 39% of our sample required consumers to agree to unnecessary uses or disclosures in order to transact. We couldn't be sure because the policies were unclear.

On individual access, over a third of the companies to whom we sent requests failed to respond at all. Of those that did respond, most failed to answer all three questions we asked. Only 21% fully complied with PIPEDA's requirement to answer these questions.

Our compliance study was conducted in early 2006, five years after PIPEDA came into force. Surely five years is an ample grace period for companies to get compliant with these pretty basic obligations. So why such a high rate of non-compliance?

I think there are two reasons:

First and foremost, there is no real incentive for companies to comply with PIPEDA. Second, the Act's provisions on notice and consent are unclear.

Something needs to change in the enforcement of this legislation. Companies have to believe that they risk significant reputational or financial damage if they don't comply. That is simply not the case now. Even reckless and wilful violators get away with, at most, a private admonishment from the Privacy Commissioner.

We have made a number of recommendations to rectify this situation, most of which do not require any major change to enforcement regime. Although we think that the Commissioner should have order-making powers, there are a number of other amendments that could collectively create the kind of incentives that industry needs. I refer you to our recommendations # 3 to 11 in our written submission.

Another possible reason for some of the non-compliance we found is that certain of the Act's obligations are unclear. Notice and consent requirements, in particular, are poorly drafted. I take some responsibility for that – but remember, the CSA Code was drafted as voluntary code, not as legislation. I think I can safely say that no one on the CSA Committee ever expected that it would become law as drafted.

Alberta and B.C. have done a much better job of articulating the obligations that PIPEDA meant to convey, and we therefore recommend a redrafting of PIPEDA's consent provisions along the lines of the Alberta legislation.

Our study also exposed strange gaps in the Act that limit its effectiveness. For example, there is no clear requirement to advise people as to how their information will be used. There is no requirement for organizations to disclose the source from which they got your information. And there are no special limitations regarding collection of information from children, whose credulity and ignorance can be easily exploited by commercial interests.

We have provided you with recommendations addressing all of these gaps and drafting issues.

I don't have time to cover the rest of our recommendations, but let me briefly mention data breach notification. Over the past year, CIPPIC has been leading a multi-researcher project on identity theft, funded in part by the banks. Identity theft strikes relatively few unlucky individuals, but when it strikes, it can be devastating. And its incidence seems to be growing.

There is nothing in PIPEDA that requires organizations to inform affected individuals of security breaches that make them vulnerable to identity theft. And there is little incentive for organizations to expose their faults voluntarily. We need a legislative requirement for organizations to notify individuals when their data is exposed to potential abuse.

CIPPIC has researched existing Canadian law on data breach notification, the various approaches being taken to this in the US, and the arguments for and against. We will be publishing a White Paper with detailed recommendations on the issue before Christmas, and would be happy to share it with you.

Thank you for your time. I would be pleased to answer any questions.