

Oral Remarks to the
House of Commons Standing
Committee on Access to Information,
Privacy and Ethics

Murray Long
February 6, 2007

I wish to thank the Committee for inviting me here today.

I am a self-employed privacy consultant who has been living and breathing PIPEDA since the bill was introduced in Parliament back in October 1998.

As my resume states I am something of a privacy law expert and I am willing to attempt to answer any questions you may have about the law and give you the best insights I can. I look forward to having a dialogue with you and addressing, to the best of my ability, any aspect of the law or how it works in practice

PIPEDA is important legislation. It establishes a fundamental right to privacy in the commercial marketplace and it sets out a framework under which the interests of citizens in controlling their personal information are balanced against the needs of businesses to collect, use or disclose it for legitimate and reasonable purposes.

By and large, this balancing of interests works well and, by and large, PIPEDA is a good law. In fact, as someone who helped write the CSA Code that forms Schedule 1 of the Act, I have found it quite remarkable that these 10 principles have been so durable and have stood up so well to the test of time. Despite the lack of clarity in some of the wording and the legal nit-picking that goes on at times, the broad concepts are solid and provide a basis for reasonable people to make reasonable judgments about how personal information should be protected.

This review process is nevertheless a very important opportunity to fix some problems with the law and make it even more effective - more efficient for business in some regards and more fair for the public in others.

To comments that have been made that it is too soon to hold this review, I disagree strongly. There are problems that need fixing right now on the basis of six years of application of PIPEDA, the insights gained from next generation laws of Alberta and BC and growing public concerns about such problems as identity theft. The work you are doing right now will have a very major impact in making PIPEDA even better legislation for the future.

I have been watching intently the comments of other witnesses who have appeared and I have decided at this juncture to restrict my formal comments to addressing seven issues. I think they are all important issues, some of which have not received much attention yet, and I would be pleased to talk to any of them

Of these, in my oral comments, I am going to speak about three of them.

The first is breach notification. As my submission notes, identity theft is a major problem and it affects the entire marketplace, even responsible companies that have strong data safeguards and have never encountered a breach. The costs of security breaches and identity theft in particular are borne by the marketplace and result in higher costs to goods and services and as importantly lead to diminished public trust in data sharing.

Responsible companies may believe that breach notification rules should be left up to them - and I have no doubt that responsible companies will act responsibly in this regard, mindful of reputational risk, fiduciary responsibilities and so on. However, as Canadian Marketing Association President John Gustavson observed years ago when he advocated for a privacy law, not privacy self-regulation, the world is not all made up of responsible companies.

There needs to be a mechanism that will enforce responsible behaviour, especially in this particular area.

In looking at the mechanics of a breach notification requirement, I have proposed a four point model which I think is clear, fair, strong, realistic, and protects the public interest.

This model is that the duty to notify must apply to all sensitive information, not just financial records. A breach of health records, for example, can cause great personal distress and have grave consequences for people's lives.

An organization would continue to have discretion to determine the significance of a breach and notification requirements, but must apply an objective reasonable person test in doing so

They must notify the Privacy Commissioner where a reasonable person would consider it appropriate to do so and must make this notification in a short, legally prescribed time frame following discovery of the breach.

Where they notify the Commissioner, they must describe the breach, efforts taken to contain it, efforts taken to mitigate the impacts, and what decision was taken to notify affected persons, and if no notification was made, explain the reasons why not. The Commissioner could then question these decisions.

The important point in all of this is to have enforcement tools. I therefore propose that a failure to notify the Commissioner as I described would be an offence under the Act with similar penalties as other offences.

To further back-up enforcement, the Act should state that whistleblower rights specifically apply where employees notify the Commissioner about a breach.

I think this proposal is solid and it bears your consideration.

My second point deals with consent in the employment context. I have seen enough evidence, through PIPEDA complaint findings, to satisfy myself that the requirement for employee consent for new purposes that are reasonable ones in the workplace imposes a huge administrative burden on organizations and can and does lead to situations where employees, exercise a right to refuse consent, and can do so in an arbitrary manner, for what are justifiable information collection purposes.

The Alberta and BC laws foresaw this problem and wisely removed the requirement that consent be required in the employment relationship, moving instead to a standard where purposes must be identifiable and purposes must be reasonable. I have seen no evidence to indicate that this Alberta and BC model does not work well or that any real privacy rights of employees in the workplace are trampled as a result.

I undertook a very detailed analysis of consent issues in my submission to the Commissioner's review process and would be pleased to provide Committee members with a copy of this, if they so wish.

My final oral comments are reserved for a matter that has not received adequate attention so far during this review.

That is the way in which the *Public Safety Act, 2002* amended PIPEDA to permit private sector organizations to collect new information about customers or employees or any other party on their own for purposes related to national security, the defence of Canada or the conduct of international affairs, or do so at the request of a national security agency.

In making these amendments, which were added in the wake of 9/11 and the heightened concern for public security, PIPEDA enters a very different sphere than normal commercial business activity.

With these amendments, organizations can, on their own, or at the prompting of the state, undertake the type of information collection that is normally undertaken only by state agencies, and where our society has recognized the need for the highest level of constitutional protections under the *Charter of Rights and Freedoms*.

With these amendments, because they enable a business to collect new information about a person on the suspicion of a security threat or do so at the request of the RCMP or other security agencies, there is a great risk that *Charter* rights could easily be offended.

As you know, private businesses are not subject to the *Charter* and, in some cases, may have little knowledge or awareness that *Charter* rights and could therefore collect information that might constitute an unreasonable search under Section 8.

Moreover, if private companies are co-opted by security agencies to collect such information on their behalf, there is a further risk of such agencies using PIPEDA to do an end-run on their obligations to uphold the *Charter*.

In my written submission, I have made the effort to explain in great detail the nature of my concerns. This is a complex issue, but I hope you will take the time to read these detailed comments and to consider them carefully.

I must stress that I am not a lawyer and not schooled in the intricacies of constitutional law and *Chatterrights*.

However, as a privacy consultant who studies the details of PIPEDA carefully, I was struck the moment I saw the new amendments made via the *Public Safety Act* that there was a grave and quite real risk that *Chatterrights* - firstly section 8 and possibly section 7 - could be violated if such collections of information ever took place.

As constitutionally protected rights are at issue here, I urge the Committee as a matter of public duty to give this the attention it deserves and recommend in its report to Parliament that the Government reconsider these amendments with a view to removing them from the Act.

Thank you for giving me the opportunity to present my views. I look forward to your questions on this and any other topics.