

BOWLEY KERR COLLINS

BARRISTERS, SOLICITORS, PATENT AND TRADEMARK AGENTS

NEWSLETTER

Number 21

<http://www.lawteam.ca>

September 2003

Getting ready for PIPEDA: what you need to know (and do) before January 1, 2004

Excuse me? What's a PIPEDA? The *Personal Information Protection and Electronic Documents Act* is intended to give Canadians privacy rights with respect to their personal information collected, used or disclosed by a private-sector organization.

What, me worry? You should. Get it wrong and you can face \$100,000.00 fines, punitive damages of up to \$20,000.00, and the embarrassment and business interruption of an investigation.

Yeah, but it's designed to reign in the big banks and telemarketers and everybody who's going to play fast and loose with my info, right? Well, sort of. But it applies to *everyone* who collects and uses personal information-- realtors, medical offices, churches, clubs..... The individuals who make up these organizations must "do it right or else".

You have my attention. What do I need to know? In brief, understand your responsibilities as a business person or as a board member of a church, synagogue or charity. Even as an employee, you have responsibilities.

OK, so gimme the skinny. Here are the Act's "10 principles" regarding personal information (PI):

1. Accountability: You are accountable for the PI under your control.

2. Identify Purposes: Before collecting PI you must identify the purpose for which you are doing so.

3. Consent: Have the informed consent of the individual before you collect his or her PI.

4. Collection: The collection of PI shall be by fair and lawful means, limited to what is necessary for the purposes identified.

5. Use, Disclosure, and Retention: PI shall not be used or disclosed for purposes other than those for which it was collected, except with the individual's consent or as required by law. It may be retained only as long as necessary to fulfil those purposes.

6. Accuracy: PI shall be as accurate, complete, and up-to-date as necessary for the identified purposes.

7. Safeguards: PI must be safeguarded in a manner appropriate to the sensitivity of the information.

8. Openness: Specific information about your PI management policies must be made readily available to the individuals.

9. Individual Access: You must inform anyone, upon request, of the existence, use and disclosure of their PI and give them access to it. They may challenge its accuracy and completeness and have it amended as appropriate.

10. Challenging Compliance: An individual shall be able to challenge your compliance officer concerning compliance with these principles.

For more complete detail, see the online guides at: http://www.privcom.gc.ca/information/guide_e.asp

Please call us if you have specific compliance concerns with respect to your organization.

I do not object to people looking at their watches when I am speaking. But I do strongly object when they start shaking them to make sure that they are still going.
---Lord Justice Birkett

Creditor-proofing reminder-- for most business and professional people, a very simple and effective form of creditor-proofing is to maintain most family assets in the name of the other spouse. Timing, however, is everything-- you have to fix the roof *before* it rains!

What do you get when you cross the Godfather with a lawyer?

An offer you can't understand!

BOWLEY KERR COLLINS
NEWSLETTER

Number 21

<http://www.lawteam.ca>

September 2003

He who is kind to the poor lends to the LORD, and he will reward him for what he has done. *Book of Proverbs 19:17*

Who gets it done? Who makes it fun? This summer it was Madiha, our co-op student, and Meghan, fresh back from Ireland. Also thanks to Trinden who keeps our network humming, and Steve who got our new phones up and working beautifully. We also welcome Cass Bowley to litigation support and say good-bye and offer best wishes to Moji Akpata, who recently completed her articles with us.

"I would rather be exposed to the inconveniences attending too much liberty than to those attending too small a degree of it."
-Thomas Jefferson

Grosse v Purvis This recent Australian case may soon prove important to Canadians. Like Canada, Australia's courts have for years been saying that *maybe, probably, perhaps* there is a right of action for invasion of privacy, but have not addressed the question squarely. In *Grosse*, the District Court of Queensland had a clear and obvious set of facts in front of it. The court "took the plunge" and said that it's about time to declare that wilful and blatant invasion of privacy will not be tolerated and awarded damages of A\$178,000.00.

Given that Canadian law is today in almost exactly the same state as was Australia's immediately before *Grosse*, it is a safe bet we will follow suit.

The most wasted of all days is one without laughter.
e.e. cummings

e-counsel

Legal and strategic advice for e-business

"Beyond Fear": Essential Reading for e-Business (and every business and every home)

Bruce Schneier is one of the gurus of internet security and author of various texts on cryptography and systems security. "Beyond Fear", however, discusses in a general way the root concerns of all security questions, whether they be securing a building, an airport, a network or a nation. He deals realistically with the politicians who must be seen to be doing something, as well as the security professionals who profit from an aura of black magic and suggests five basic questions which reduce every security issue to common sense:

1. *What assets are you trying to protect?*
2. *What are the risks to these assets?*
3. *How well does the security solution mitigate those risks?*
4. *What other risks does the security solution cause?*
5. *What costs and trade-offs does the security solution impose?*

With this analysis, Schneier looks at how we as a society approach security. Sometimes we get it right, but all too often we get it wrong, spending a fortune to bark up the wrong tree. This leaves us in the worst of all situations—lulled into a sense of false security with fresh vulnerabilities inviting the attacker. National ID cards, electronic voting and massive personal information databases promise to make us safe against terrorists and other bad guys, but on deeper analysis serve only to erode our freedoms while giving little in return.

Combining a common-sense approach with a philosophical examination of trends in Western society, Schneier is neither "left wing" or "right wing". In a world filled with Chicken Littles and neo-Mussolini's, his text is refreshing news: we can, and we must, think our way through security problems.