

House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) - Meeting, Nov. 29, 2006 (Chaired by Tom Wappel)

Notes taken by Tara Berish, CIPPIC Articling Student

**NB: This is not a transcript. We do not guarantee accuracy of these meeting notes. For a transcript of the meeting, see the Committee website.

Witnesses:

- David Loukidelis, Commissioner, Office of the Information and Privacy
Commissioner of British Columbia
- Valerie Steeves, Department of Criminology, University of Ottawa.

Valerie Steeves, University of Ottawa:

- Privacy-related concerns: Surveillance cameras in stores, children online, RFIDs
- People/consumers are automatically disclosing information without knowing it
- The environment is set up to collect information for commercial purposes, but this information gets disclosed for non-commercial purposes as well
- “Neopets” website – top website for children
 - Children are supposed to register and provide all kinds of personal information about themselves
 - The website looks like a playground, but is actually doing market research
 - Children earn neo-points by filling out marketing surveys, which include questions like “what do your parents do?” or “what products do you prefer?”
 - Some of the products presented include beer, cigarettes and cigars
- Facebook – social networking website
 - Encourages the posting of personal information (including such details as sexual orientation and political views)
 - It records everything, including chats, and matches it up to other information it finds in cyberspace, including blogs and newspaper clippings about the poster
 - Facebook states that by posting on it, you are giving it a non-exclusive license to your information
- Recommendations:
 - 1) Principle 4.3.2 – Make it clear to companies that they must explain what they will do with personal information on or before a person consents to its collection
 - 2) Clarify guidelines with respect to types of consent (express, implied, opt-out etc.)
 - 3) Privacy policies need to be fixed – require that they be written in plain language
 - 4) Require specific definitions of the purposes of collection
 - 5) s. 5(3) should state that the purposes should be reasonable *to the consumer*
 - 6) Principle 4.3.3. – Make it clear that a business can only refuse to deal when the information in question is necessary to the completion of the transaction at hand
 - 7) Amend s. 3 to state that privacy is a human right, and a social and democratic value. It should outweigh the business practices when they are in conflict.

David Loukidelis, B.C. Privacy Commissioner :

- Speaking on his own behalf, not *as* Commissioner in B.C.
- In Canada we have the challenge of a multiplicity of privacy laws. People say this is hard for businesses to manage. This is not true – the laws are substantially similar.
- The B.C. privacy legislation is generic, and covers the public and private sectors
- There has been 3 years of experience with the B.C. legislation now
- Under B.C.'s PIPA, work product was carved out of the protections in order to exempt from protection information that is not about individuals
 - The intent was to ensure that an employee can't ask for every email produced etc. after he or she has left a company
 - The definition could be difficult – especially with respect to workplace monitoring
 - Employee's personal information is in a special category. You don't need consent to collect it if it is only used to establish, maintain or terminate employment
 - Consent to workplace surveillance is not to be expected, which is why there is a carve-out to cover such things as suspected fraud
- Business transactions – to permit parties involved in the prospective sale of a business...you need to notify customers in B.C. when there's been a change in control of a company

Questions and Answers

Comments and Frequently Asked Questions

- Mr. Loukidelis oddly suggested that there should be no duty to notify of a breach of security with respect to personal information in the B.C. PIPA. He also suggested that his order-making powers were not particularly useful.
- The Committee seemed quite sceptical about many of Ms. Steeves' claims. They appeared to think she was exaggerating, and questioned her conception of privacy as a human right.
- Once again, concerns about small businesses were raised several times, as were questions about work product and the health care industry.

Dhaliwal: We live in a knowledge-based economy. How far can we go in balancing interests and still keep businesses going?

Steeves: The mechanisms used to collect information obfuscate what's going on – we need to be able to make our own choices. 70% of all ID fraud comes from insiders collecting our information. Individuals need more information.

Loukidelis: Ms. Steeves is not saying we always need more legislation, but we should not proscribe/prescribe particular technologies.

Dhaliwal: Won't we always have privacy problems? How are these things working in the public sphere?

Steeves: Public privacy was a democratic impulse. Now, public bodies can get information from commercial collection, so protection in the private sector has become more important than ever.

Lavallée: I was amazed by Ms. Steeves's presentation. Not all of this is going to happen. To what extent do we have to have laws for things that might never happen? These technological measures are expensive, and labour intensive. Also, isn't regulating the Internet too hard? Should we be prohibiting cookies? Finally, in Quebec, there are laws against advertising to children. Are there such laws elsewhere? How could we put this into the legislation? Should we really be prohibiting surveys? Individuals can decide for themselves whether or not to take a survey. What do you have to say about privacy as a fundamental right?

Steeves: There are voluntary codes with regards to advertising to children elsewhere. There are children's social networking websites. Children as young as 13 use these. We have to look more carefully at how we define advertising. Legislation shouldn't be technologically sensitive – we just need to make sure there's notice and consent. What about PIPEDA is not working here? We have to get back to basics. We probably don't need to prohibit cookies to do that. I might want that marketing, but I should get to decide. Now the company decides what purposes are appropriate, as well as whether or not I consent. For example, I get messages on my phone about 30 times a day, for which I pay over a dollar every time. I don't know who has my information.

Loukidelis: General principles are better than technology-specific ones. There's software that will help you control cookies.

Tilson: Questions re: work product.

Loukidelis: Answer re: work product

Tilson: How much should the state interfere with the selling of information during a business transaction? Non-disclosure is a routine clause in these contracts.

Loukidelis: The B.C. legislation facilitates transactions.

Tilson: Surveys... Don't we ever have to take control of our own actions? Shouldn't we just train our kids not to give out information? Can the state go too far in interfering with people's lives?

Steeves: The legislation is set up to require consent, in order to allow people to make those decisions. The problem is that information is often released in social situations where people don't realise it.

Tilson: What if you have a law that says you can't survey kids? I have a problem with saying that adults can't answer surveys.

Steeves: We do have provisions...

Tilson: What should the penalty be?

Steeves: That's what we've got in PIPEDA.

Thibeault: I understand the technology-neutral approach, but there are many technologies which are impossible to control. But maybe we have to consider the technologies specifically, because everything is changing so quickly. I don't like that they ask for my information to buy electronics. But there are things that are in the interests of society, like healthcare. It seems reasonable that doctors and pharmacists should know my whole health history. Not everyone agrees.

Loukidelis: There's a big investment underway with respect to health. I can't say where the balance lies.

Steeves: PIPEDA covers the flow of medical information. We need to recognise the value of health information in the marketplace. Pharmacies profile doctors to sell products. There are secondary purposes and unintended consequences. People respond by lying, hiding and not going to the doctor. When we allow the information to flow and don't respect the social value of privacy we will have these unintended consequences.

Stanton: The B.C. legislation has order-making powers. Comment on the ombuds model.

Loukidelis: Order-making power is not the tool of first choice. We first try mediation (88-91% of cases are settled by mediation). Only 7 binding orders were issued. We can also refer individuals to the companies, to other processes, to the Human Rights Tribunal. We use educative powers. So, order-making powers are the last ones we reach for.

Stanton: The OPC rarely uses the Federal Court. Should we be looking at a departure from the ombuds model?

Loukidelis: It's not as if the ombuds model doesn't have sharper tools.

Laforest: Does the fact of your having these powers (as well as others) make the process better or worse?

Loukidelis: This is only an impression – but the fact that there's an order-making power might encourage complaints, not discourage them. The possibility of an order may concentrate the minds of organisations. Once they know their obligations, they may try to resolve things earlier. There's good compliance under the federal legislation, I think.

Lavallée: You were talking about fundamental rights. Don't you need information sometimes, no matter what?

Steeves: Privacy has been recognised in Canada as a human right. That doesn't mean we don't have to balance it against competing rights – if you can recognise it as a fundamental right in PIPEDA, you can't balance it against commercial interests – only real rights.

Wallace: For Loukidelis – if there's a breach, does the legislation in B.C. require notification?

Loukidelis: No. Our legislation is up for review. I would not support mandatory notification like in the U.S. But we should continue the way we're going and focus on education.

Wallace: National businesses incur no costs to having to abide by different laws everywhere?

Loukidelis: The similarities in the laws across Canada are more than the difference. There are nuances, but they're not onerous.

Wallace: Question about employee privacy.

Chair: You are conducting a review of the B.C. Act next month – are there any major issues that will come up which are relevant to us?

Loukidelis: I will provide you with some materials – the committee is not yet struck.

Dhaliwal: Question re: health information.

Chair: Question re: work product.

Stanton: The laws are scaring small business. Are we at a threshold where we need to be developing a whole new set of laws?

Steeves: PIPEDA was a balance – the laws need to be tightened up. Compliance has been an issue because there hasn't been enough education yet.

Stanton: So you think we're in an evolutionary process – we don't need a total overhaul?

Steeves: We need a new conception of privacy as a fundamental value, not just in PIPEDA.

Chair: Can you give us your comments on the unauthorised disclosures to the U.S. and the amendments which came out of that. Also, why did the amendments only refer to the public sector?

Loukidelis: There's a distinction between the public sector, where there's no possibility for consent, and the private sector where you can essentially vote with your feet.

End of meeting