House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 020 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Wednesday, November 29, 2006

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Wednesday, November 29, 2006

● (1530)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): Good afternoon, ladies and gentlemen. I'd like to call the meeting to order.

Pursuant to the order of reference of Tuesday, April 25, 2006, and section 29 of PIPEDA, we're involved in a statutory review of part 1 of the act.

Today we have, from the Office of the Information and Privacy Commissioner of British Columbia, Mr. Loukidelis, the commissioner himself; and as an individual, Valerie Steeves, from the Department of Criminology, University of Ottawa.

Welcome to you both. I'm guessing that you'll each have an opening statement. I think what we'd like to do is have you both give your opening statements, and then we'll go to questions.

Ladies first? Valerie Steeves, please.

Ms. Valerie Steeves (Department of Criminology, University of Ottawa, As an Individual): Thank you very much for the opportunity to come to speak with you this afternoon.

As I was preparing my comments for today, I was surprised to go over the transcripts yet again and read that both Mr. Binder and Commissioner Stoddart indicated that PIPEDA is working quite well and that the community is generally satisfied with its provisions.

One of the hats I wear is as the chair of the National Privacy Coalition. It's a loose coalition of over 100 privacy experts across the country. We facilitate and support communication on a number of issues. We also provide platforms for organizing around those issues. I think it's quite apparent that the privacy community, in any event, has some serious concerns about the ways in which PIPEDA has been protecting, or perhaps failing to protect, the privacy of Canadians over the past five years.

As early as November 2004, the Public Interest Advocacy Centre issued a report that concluded that the legislation was in fact “a sheep in wolf's clothing”. I know you're aware of the report that was issued this year by the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa that documented widespread lack of compliance on the part of the private sector. I know from my own work with the small-business community, particularly in the context of public education, that there's a widespread confusion in a large part of that community about their responsibilities under the act.

From a consumer's point of view, I fear that for all of PIPEDA's good intentions, perhaps the best way to describe it is “death by a thousand cuts.” The language in the act is vague. Many of the rights and responsibilities set out in the legislation are either poorly defined or not defined at all.

That vagueness isn't an accident. The CSA code that the act is built on is a consensus-driven document. When consumer rights and business practicalities conflicted around the table when the CSA negotiation was going on, the drafters intentionally used language that could be interpreted broadly by both sides. That makes perfect sense when you're talking about a voluntary code, but it's disastrous for legislation.

Is PIPEDA fixable? Well, yes, with some caveats. First and foremost, I think we need to recognize right up front that the act is trying to do two very different things. On the one hand, it purports to protect individual privacy rights; on the other hand, it's designed to promote electronic commerce and make private information available in the marketplace for commercial purposes.

Those two purposes aren't always reconcilable, and I think you see a number of problems arise when you look at the kinds of platforms that have been developed to support electronic commerce.

First of all, a number of the technologies that are rolling out in the e-commerce world are built to allow the invisible collection of a whole range of personal information about you, about me, about all of us.

You know, for example, that cookies can track the websites you visit. Microsoft is one of many companies that use web beacons. Web beacons are these single-pixel graphics. They're so small that they're invisible, and you can pop them on a web page or stick them in an email. They're used there because the companies want to be able to track what you do when they email you. This little beacon will let them see if you, if I—

If I'm on MSN and am doing instant messaging—I'm registered there, and they know who I am—they pop one of these little web beacons into the emails they send me. They can then check and see what Val's up to. Did she read our email? Did she click on any of the links? They also have an arrangement whereby they have web beacons imbedded in the websites of their advertisers to see whether Val goes over to one of the sites and buys one of the products they were advertising.

It's not only me they're watching—I'm rather boring. It's particularly important to realize that over half of Canadian kids between the ages of nine and seventeen instant-message on a daily basis; that's over 50%. An additional 20% instant-message at least every other day.

They can put a camera in a store, for example, to track eye movement. If I go into a store wanting to buy a pair of jeans for one of my kids and happen to notice a red sweater over in the corner and keep checking it out, the camera is set up to collect all that information about me. This can alert the store manager, so that the store manager can send over a clerk to close the deal on the red sweater that I did not come in to buy.

I understand you've been talking a bit about RFID tags. RFID tags are increasingly being implemented or deployed throughout the electronic marketplace. These are the promiscuous little devices that are attached to the products we buy. They're designed to do one thing: to tell whoever asks them who they are and where they are. If any RFID reader asks, they're promiscuous, and they'll say "Here I am, I'm right over here."

● (1535)

I've tried, and it's very hard to tell if these things are actually attached to the products I buy, but it's virtually impossible to tell if they're turned off when I leave the store. Now, as an individual consumer, I'm not just worried about the information I'm dropping as I go through the electronic marketplace; I have to worry about the fact that my things are leaking information about me as well.

When you think about the information flows in this environment, people who shop this way, people who participate in electronic commerce are automatically—not by choice, but automatically—disclosing personal information just by using a free instant messaging service, buying some razor blades, or walking in front of a store's cameras. Since that collection of information is invisible, is seamless, it's really difficult for me to even realize it's there, much less to contest it.

Secondly, the environment is set up so that a lot of the information collected about individuals and used for commercial purposes is actually disclosed for non-commercial purposes. We're just going through our daily lives. We could be playing, we could be chatting with friends, we could be surfing the net, or we could be walking through stores and looking at red sweaters for fun. I'm not necessarily asking a company to enter into a transaction with me when this information is collected. In fact, the company is watching me as I go about my private life and is collecting information about me for its own purposes. I'd like to give you a couple of examples, so that you can see how this plays out in the information marketplace.

Neopets is one of the most popular e-commerce sites with Canadian kids aged nine to thirteen. Like almost all the top fifty sites that Canadian kids hang out on, they're encouraged to register. That means they are asked to provide their real name, their e-mail, their age, their gender, and some form of location information, whether it's a real-world address or a postal code. When kids go on this site, it looks like a playground, but it's actually a market research firm. The kids get there and they want to play, and they have an opportunity to create this virtual pet, a Neopet. In order to keep their Neopet alive, they have to buy food for it. There were a number of complaints, so they now have a Neopet food bank so they don't starve, as they used to in earlier years.

Some hon. members: Oh, oh!

Mr. Mike Wallace (Burlington, CPC): It must have been the Liberals.

Some hon. members: Oh, oh!

Ms. Valerie Steeves: The nanny state rules again, right?

When kids go to Neopets and have to buy these things, they have to first earn Neopoints. The way they do that is by filling out marketing surveys. These surveys contain questions that I think you'd expect. A couple of years ago I filled out one about whether or not I liked breakfast cereals. It asked me, "Do you eat breakfast? How often do you eat breakfast? What time do you eat breakfast? Do you recognize this particular brand?"

But these surveys also ask questions that I think will surprise you. The one I filled out asked me what my parents did for a living. "Does Mom work outside of the home? What kind of car do your parents drive? How much money do you think your parents earn a year? Here are some brackets."

Then they said, "We really want to know more about you. This is empowering. You can tell us so much about yourself and we'll be able to make this site even better to suit you better. Why don't you look at this list of fifty things and click on the things that really turn you on?" The list again included things that you would expect, like Barbies, video games, and reading. It also included things I don't think you're going to expect. On the list was beer, alcohol, cigarettes, and cigars.

These kids are nine and they are playing. They are not disclosing information for commercial purposes. Yet the kind of legislation that we have in place lets companies set up these kinds of environments and, through a very weak consent mechanism, capture that information and reconfigure it as a commercial commodity.

Social networking sites like Facebook, for example, work in much the same way. It's particularly popular right now with Canadians in their twenties and early thirties. These kinds of sites encourage people to post all sorts of information about their personal lives. You put your pictures up, you have your list of friends, and you fill out personal profiles. The profiles ask you to disclose things like your sexual orientation, your political views, and your religious views.

● (1540)

The company takes all this information and then also records all of the messages, all of the chat you have with your friends, all the searches you make, and all of the parties you set up. Then it takes the additional step of matching all that information about you with information also about you from other sources, like newspapers, blogs, instant messaging. The idea is to take it, slice it and dice it, and then sell you back to advertisers.

When people are on the site, they think they're sharing photos with their friends. My 20-year-old grad students, for example, spend a lot of time hanging out on Facebook and they throw up all of their pictures from their different parties, complain about how bad their classes are, gossip about their professors, but that information is encaptured as a commodity.

In fact, Facebook is one of a growing number of companies that now in their agreement say you've given us, just by using our service, a non-exclusive license. We now own that stuff and we can do what we want with it. We can give it away. We can post it in other places. In effect, what they're doing is they're taking the intimate details of these Canadians' private lives and turning them into the company's intellectual property.

The Chair: Excuse me.

Normally we allow the witness to give us a ten-minute opening statement, and you're at that stage. I'm wondering if you could wind up with a recommendation or suggestion that the committee should consider. And then these examples that you give, which are all very interesting and reconfirm for me why I don't use the computer, could come out in questions.

Ms. Valerie Steeves: Actually, that's exactly where I am. I have seven recommendations that I'd like to leave you with. They're very doable and they're very practical.

The first one is that if you want to make sure people know how their information is being used so they can make reasonable and informed decisions about whether or not they want to use the computer or disclose this information, I'd suggest you should amend principle 4.3.2 to make it clear that companies have to tell people what they're doing before obtaining their consent. Again, you can look to the B.C. and Alberta legislation, because they've had the opportunity to look at a number of the weaknesses in PIPEDA and come up with tighter language.

Secondly, I'd suggest you clear up the loopholes that let companies assume people have consented, and provide specific definitions of expressed, implied, and opt-out consent.

Thirdly, one of the main practical mechanisms to ensure that people know what's going on in the information marketplace is the privacy policy itself. According to all the research that's come out, privacy policies have typically been written in incomprehensible language that does little to actually tell the individual how or even when her information is being collected or used.

Just to quickly make this point, I'm doing some work right now on how to improve the comprehension of privacy policies, and my colleague, Jacquelyn Burkell at Western, said her research assistant couldn't understand something. She said, “Here's a policy from one of the sites Canadian kids hang out on the most. Can you just tell me, what do they collect, how do they use it, and how can somebody opt out of this?” It took me nine hours to answer those questions, and for what it's worth, I have a law degree, a PhD in communication, and 15 years' experience in privacy law.

So I would suggest that you should consider amending the act to require that privacy statements are written in plain language so that individuals know exactly what information is being collected and how that information is being used.

Similarly, I would suggest that you look at the way the act allows corporations to define purposes. Facebook, when it's negotiating consent with people, says they collect all this information “to provide you with more useful information and a more personalized experience”. I would suggest we should amend the act to require specific definitions of purposes.

FIfth, you know that the purposes for which a corporation is allowed to collect information are required to be ones that a reasonable person would consider to be appropriate in the circumstances. The big question is, reasonable for whom? For the corporation or for the individual? I would suggest it makes perfect sense for Neopets to want to figure out if my kids are interested in alcohol, but from a consumer point of view, that is not a reasonable request.

So I would suggest you consider amending subsection 5(3) to read something along the lines of organizations being allowed to collect information for purposes that a reasonable consumer would consider appropriate in the context of the immediate transaction. And ultimately, often what happens in the marketplace is that consumers are left with a take it or leave it response from a corporation: This is what we do with your information. If you don't like it, go away.

I would suggest that to strengthen the act in this regard, you revisit principle 4.3.3, which talks about tied consent or the refusal-to-deal provision, and make it clear that a company can refuse to deal with someone only if they do not give them information that's necessary to provide the goods or services that are involved in the transaction. And again, you can look to the Alberta or B.C. legislation for precedents.

Lastly, and perhaps most importantly, I would ask you to carefully consider which side of the line you'll come down on when business imperatives conflict with privacy, because they will conflict with privacy.

I would ask you to consider amending section 3 to make it clear that privacy is a human right, a social value, and a democratic value, and that the purpose of PIPEDA, its primary goal, is to protect the privacy of Canadians in the electronic marketplace that I've described to you.

Thank you very much for your attention.

● (1545)

The Chair: Thank you, Professor.

Before we go to the commissioner, did you buy the red sweater?

Ms. Valerie Steeves: No. I don't even like red.

The Chair: Commissioner, we're looking forward to hearing what you have to say. Welcome. Please go ahead.

Mr. David Loukidelis (Commissioner, Office of the Information and Privacy Commissioner of British Columbia): Thank you very much.

Thank you, Mr. Chair, members of the committee. I appreciate the opportunity to travel to a warmer climate to be with you today, and share some views on the British Columbia approach to and experience with private sector privacy legislation in the last three years.

Of course my remarks today are directed to the situation in British Columbia, to the legislation we have there. I don't propose to take it upon myself to recommend to others what is appropriate or not appropriate in any particular jurisdiction's legislation. I trust it goes without saying that I'm here on my own behalf, if you will, on behalf of my office, as opposed to on behalf of the British Columbia government.

By way of introduction, I'd like to make a couple of general comments about the fabric of private sector privacy laws across this country. I think it's important to emphasize that beginning in 1994, with the initiative in Quebec, which responded in part to developments in the European Union, Canadian legislators have enacted in fact a fabric of private sector privacy laws, as opposed to a patchwork.

It has sometimes been suggested that in Canada we have the challenge for private sector businesses and other organizations of dealing with a multiplicity of private sector privacy laws that make it difficult to do business in this country. I would, to the contrary, argue that in fact the laws in Canada are not only consistent but indeed substantially similar. They are that way because they all incorporate what are known as internationally accepted fair information practices, which are reflected in international instruments such as the OECD guidelines on transborder data flows and in the more recent APEC privacy framework of 2004.

The situation, then, in Canada is that although we have a provincial law in, for example, British Columbia, that governs the entire broad private sector, all organizations in the private sector that are provincially regulated in British Columbia are covered by our Personal Information Protection Act. Although we have legislation in Alberta, Quebec, and federally, those laws really are of a piece, I would argue, and any concerns around the challenge to businesses and other organizations presented by having different laws are, in my view, if not misplaced, perhaps at the very least somewhat exaggerated.

In any case, as I've said, the legislation in British Columbia is a generic private sector privacy law; it covers all sectors of the economy that are provincially regulated. The for-profit and not-for-profit sector, some 350,000 organizations in British Columbia, have, since January 1, 2004, been subject to the rules that are generally described as fair information practices internationally. So our office has some three years of experience with that legislation, and my purpose today is to share with you some general observations about some selected issues that I know have been of interest to the committee in previous proceedings in its statutory review of the Personal Information Protection and Electronic Documents Act.

The first specific issue I would like to address that is tackled in British Columbia's Personal Information Protection Act—which I'll refer to as PIPA—is work product information. I wanted to deal with that first because it is something that I know has been of interest to the committee. There was a considerable amount of attention given to it in your session on Monday, so I thought perhaps I might, anticipating that the committee may have heard enough about that, and subject to of course the committee's wishes on this, tackle that issue first.

Under British Columbia's PIPA, a definition has been included of work product information. The intent of this is to carve out of the concept of personal information that is protected under the rules in PIPA a certain body of information that is not, in any generally accepted sense, personal information about an individual.

A similar approach has been taken through interpretation under PIPEDA federally and in certain provincial public sector access to information and privacy protection laws, but the policy-makers in British Columbia decided to tackle the issue head-on and to include a definition of work product information that they could then exclude from the protections otherwise afforded to personal information under the legislation.

The intent of this I think at its core is to, for example, ensure that an ex-employee of an enterprise cannot come to the business, after having had his or her employment terminated, and say: “In exercising my rights under PIPA to have access to my own personal information, I hereby request every e-mail, business plan, memo, fax, or letter that I ever created during my 23 years of employment with you, because of course I created them. They're in some sense about me, and therefore you have to respond to this request.” Because of the exclusion for work product information, which is information that is produced as a result of activities and responsibilities related to the individual's employment or business, the organization is in a good position simply to say no, that is not your personal information.

● (1550)

I understand that there may be concerns about how the definition is cast, a need for precision in how the definition is actually expressed in the legislation, especially when it comes to workplace monitoring. It is my view, speaking generally, that under PIPA in British Columbia, there is ample room in light of the definition that I've just paraphrased for you to actually interpret it and to ensure that workplace monitoring is subject to the appropriate regulations under PIPA and is not somehow excluded because of the definition of “work product information”.

The next issue I'd like to touch on in fact flows from that last point, and that is employment privacy and the whole issue of employee personal information. I know you've already heard how PIPEDA addresses this issue. It is a heavily consent-based statute, of course. Consent is, generally speaking, needed for the collection, use, or disclosure of personal information, including in the employment setting.

I might, as an aside, point out that PIPEDA tackles the question of employment privacy in relation to federally regulated works, undertakings, or businesses, but for constitutional reasons it has long been settled that PIPEDA cannot address privacy issues of employees in the provincially regulated workplace. That is something that PIPA does in British Columbia and that other similar provincial laws do as well.

In British Columbia, as opposed to taking the consent approach to dealing with employment privacy issues, the policy-makers decided to create a special category of information, known as “employee personal information”, in respect of which consent would not be needed. It is not necessary for an organization in British Columbia to get employee consent to collect, use, or disclose what is called employee personal information.

This is not to say that employers have free rein, however, when it comes to collecting or using their employee's personal information, because the definition of “employee personal information” stipulates very clearly that it is only the information that an employer collects solely for purposes reasonably required to establish, manage, or terminate an employment relationship with that particular individual. The legislation also imposes a requirement that any collection, or use, or disclosure of that kind of information must be for purposes reasonably related to the actual work relationship.

Instead of focusing on consent, recognizing that consent in the employment context is often coerced or that employees are under pressure to agree to employer practices, recognizing that it's not appropriate, for example, to ask an employer to get the consent of an employee who's suspected of defrauding the company to being put under surveillance—you're hardly going to get the suspect who's allegedly stealing from you to consent to that—instead of having to go through the consent route, it has been decided that you should be able to collect, use, or disclose personal information so long as it fits within the definition. So there is in fact a set of rules that does apply to personal information of the kind I've just described, and employers are therefore subject to reasonable checks and balances that appropriately, certainly in my view, balance the needs of employers and the interests of employees as regards privacy in the employment setting.

The last issue that I'd like to touch on, because I know it has come up before, is the question of business transactions. Another difference in approach under PIPA, and this is found also in the Alberta version of the same legislation, that differs from other approaches—for example, under PIPEDA—is to permit parties involved in the prospective sale of a business to share personal information of customers, employees, or shareholders, back and forth, in the first instance for the purpose of deciding whether to proceed with the transaction, and second, if the transaction proceeds, to allow that information to be disclosed to the purchaser of the business so that it can be used for the purposes for which it was originally collected, and consent is not needed in that instance.

Notice that in British Columbia you have to actually, after the fact, notify your customers, for example, that the change of control has occurred, that the business has been sold, that the assets have been spun off, as opposed to Alberta where that requirement does not apply. It may be a minor point, but it's certainly one that has widespread support in British Columbia because it acknowledges that in the context of business transactions, the due diligence leading up to them and the aftermath of the completion of the transaction, it is not necessarily either appropriate or practicable to expect parties to the transaction to obtain customer consent each time a business changes hands.

Those are essentially the issues I wanted to touch on. I suspect that members of the committee may have questions that address other issues that have come up before, and I'd be happy to answer them as best I can now or to provide you with further information if I can't assist today.

Thank you.

● (1555)

The Chair: Thank you very much, Commissioner. Yes, you are kind of lucky with the weather, or unlucky where you are—let's put it that way. I don't know how long it's going to be like this, but we might as well enjoy it.

We're going to go with our usual rounds of seven minutes, starting with Mr. Dhaliwal.

Mr. Sukh Dhaliwal (Newton—North Delta, Lib.): Thank you, Mr. Chair.

Welcome, Commissioner, to beautiful Ontario right now, because we leave beautiful British Columbia behind; and welcome, Professor Steeves.

My first question is to Professor Steeves. We're going through a knowledge-based economy right now and the technical age where the information flows so quickly. The way I was listening to you, certainly I like the red sweater, even if the store clerk comes in and closes a deal on that. To me, it might not be an issue, but to you, there's a different perspective. So how far can we go on this so that the balance is kept, to keep the businesses going and at the same time protect the privacy of the individual citizens?

Ms. Valerie Steeves: I think the legislation lays out a good framework to work with. A lot of the problems are, as I said, because the language that's used is quite vague. The problem is, if all transactions fall within this broad corporate surveillance, the individual has no way of making any decision about what happens to the flow of his or her information. So the thinking behind PIPEDA is that we need to give people enough information about what's going on so they can decide whether or not to disclose information.

Within the context of the electronic marketplace, the mechanisms we're relying on obfuscate rather than clarify what's going on. So you want to give people the opportunity to first find out how their lives will be affected if they enter into that particular transaction and to then make a choice.

I think we can go a long way just by tightening up the consent provisions and by dealing with the tied-consent provision, in particular. Once everybody starts doing it, then basically, I'm out of luck, because I no longer have the right to say no.

Let me give you an example. I walked into Home Depot earlier this month, and I was trying to return some plumbing stuff. I had bought two sizes, because I wasn't sure what was going to fit. I've had transactions with them for the past ten years. I've always been able to return things. I went in, I had my receipt, and they said, "That's fine, but first we're going to have to swipe your driver's licence." I was thinking, "Whoa!" Somebody else might be comfortable with the fact that the information is given over to them. They might even think that's great; they can match that with other information, the fact that I like that red sweater, and I will be able to get more services that I'm actually interested in. At the same time, other people might not want to, and we might have very good reasons.

Industry Canada published a report on identity theft, a discussion paper, in 2005, that stated that 70% of all identity fraud occurs because an inside employee takes that information, steals it, and gives it to the fraudster. So I don't necessarily want Home Depot to have my driver's licence in its database, because now I have no way of controlling it. It's really pretty simple: you can just say no. Right now, it's hard, the way the act is set up, because the provisions are very loosey-goosey. In fact, when I complained about this to the Privacy Commissioner's office I was told I should contact Home Depot myself and tell them I don't like their policy.

I'm not sure we're going to get the right results that way. I think we need to have a strong commissioner who is actively out there dealing with these kinds of issues and making sure that there is enough information available to individuals so they can make some kind of choice about what happens to their personal information.

● (1600)

The Chair: Mr. Loukidelis.

Mr. David Loukidelis: I don't understand Professor Steeves to be suggesting that because of risks peculiar to particular technologies, for example the Internet, we need technologically prescriptive legislative solutions. Nonetheless, I use this as an opportunity to say that, certainly for the British Columbia situation, I would strongly support the continued technological neutrality of our private sector privacy legislation, that we not try to proscribe particular technologies or prescribe particular solutions. I think it should remain technologically neutral so the legislation can grow as technologies change.

Mr. Sukh Dhaliwal: In fact, again, Professor Steeves, when you're discussing the driver's licence information or social insurance numbers or what not, isn't the onus already on a particular client to give that information to the corporations and they can hold it? You can say no, at this point in time, as well. Aren't those provisions there?

The thing is, the way I look at it, we're moving back to the aid of cases if we keep on doing this. So today it's driver's licence information, tomorrow it will be something different, right? Because with the emerging technology, all we're talking about is—

I have heard of people producing driver's licences at home now and credit cards and what not. Those issues are going to be there, irrespective of how we deal with PIPEDA. Generally, would you say that it's working okay when it comes to the public sector?

Ms. Valerie Steeves: You mean privacy legislation as a whole? Well, let me relate it PIPEDA. When you're looking at privacy in the public sector, you're looking at laws that to a large extent define the relationship between the individual and the state.

Privacy laws and access laws are actually democratic impulses. In the 1970s, people enacted them so the citizens could see what the state was doing, so they could hold the state accountable through the democratic process. Individuals would have enough autonomy that they could go about their private lives without any undue interference.

You have a funny kind of blending now. Because of the information marketplace that you're talking about, information that's captured for commercial purposes becomes available for other uses by the state. It becomes even more important in those circumstances to protect commercial privacy, because that information doesn't just stay there.

For example, I know that police officers in the northern United States have Internet-ready cellphones. When they stop you in your car because you were speeding or whatever, they can take your driver's licence and your name and pull up your commercial profile from data brokers to see what kinds of things you buy and those kinds of things.

I would make the argument that from a public policy point of view it's important to have strict controls over the uses of commercial information, precisely because as it flows into the public sector you're re-skewing the relationship between the individual and the state. One of the concerns I have is that we're now making the individual transparent to the state but using this legislation to protect governments from that accountability that was at the core of the impulse to enact access-to-information and privacy legislation.

● (1605)

The Chair: Thank you.

Our next questioner will be Madame Lavallée from the Bloc Québécois.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Professor Steeves, I was very surprised by your presentation which was bordering on science-fiction. I could hardly believe the examples you gave us, particularly with respect to the camera that tracks your eye movement when you go shopping or to that red sweater. Even if it were possible to do it, I think it would be economically unrealistic because of the high cost of technology. It would also be technically quite difficult to have is a sales clerk behind a counter looking at the sweater your eyes are attracted to.

I wonder how far we should go to amend our legislation for things that are so far out. What's your opinion on that?

You also mentioned cookies. Should they be forbidden when we know that would be extremely difficult and far from perfect? The first steps would be very difficult because they require the cooperation of more than one or two countries. Is it even possible to forbid cookies?

You talked about children registering on game sites who are being asked to answer questions. I don't know if it's the same in the rest of Canada, but we have legislation in Quebec that prohibits advertising to children. I don't know everything that's in the law but isn't there Canadian legislation prohibiting surveys directed at children? How far can we go to include these things in PIPEDA?

I always wondered about what survey firms do with their surveys. We know these firms collect information in order to sell it to others. But we can't go as far as forbidding surveys when we review these definitions. After all, people can decide by themselves whether or not they want to answer questions.

Last week, someone called me and asked how many computers I have at home. I just had my computers stolen at the office, so I refused to answer this question. I may look masochistic but I'm not.

You said you had seven recommendations. I tried to follow you as best as I could but I could only count six. I would like you to send us your documents so we can review all of your recommendations. One of them was particularly interesting and intriguing. You talked about making the right to privacy a basic human right.

Can you tell us more about this?

[*English*]

The Chair: As far as I can tell, there were four questions: How far should we go? Number two, should we prohibit cookies, and is it possible? Three, sites for kids in Quebec. And surveying kids is illegal—is it not illegal elsewhere?

She only noted six recommendations. Are there six or seven, and could you provide them in writing?

Ms. Valerie Steeves: I'd be happy to provide the recommendations in writing.

If I can answer them out of order, it is true that Quebec has legislation that prohibits advertising to children. Other Canadian provinces do not have similar legislation. There are voluntary codes in place, but having said that, it is interesting to me that the single most popular site with Quebec girls between grades eight and eleven is a site called "do you look good.com". It is a social networking site and you post pictures of yourself in this site, so other people can rate you on a scale of zero to ten. It's all about give us your profiles. Tell us what kind of relationship you're interested in. Are you straight? Are you gay? Are you interested in just a fling or are you looking for a long-term type of thing?

When you register on that site, you have to tell them how old you are, and the youngest age starts at thirteen. Like any of these other social networking sites, there's advertising built into it, but all that information is captured as commercial information, so we have to look more critically at how we define advertising.

Advertising has changed significantly in the electronic environment, and it is now driven by this pervasive collection of watching everything you do in all these different environments.

● (1610)

The Chair: Shouldn't you prohibit cookies?

Ms. Valerie Steeves: The truth of the matter is, I completely agree with David's comments. This stuff isn't technologically sensitive. It shouldn't be. We should have rules that work for us as Canadians in the marketplace. We do have rules that say if you want to collect information about me, (a) let me know, and (b) let me decide if it's okay with me.

What we need to do is see what it is about PIPEDA that's making that process muddy. Why is it so darned hard to figure out what's happening with my information in the information marketplace? I go back to the comments I made about privacy policies, about disclosures, about the way consent is obtained. If we get back to basics and look at fair information practices and take them at face value, you could give them a shot. They have the potential to put the consumer back in the driver's seat in the electronic marketplace.

I don't think you need to prohibit cookies to do that. People need to know how the marketplace grabs their information, commodifies it, and then sells it back to them. Part of that might work to my benefit. I might want to know what Apple Tunes has out now. I might want to know if there's a new product I can buy.

Most privacy advocates will agree that the problem isn't necessarily that the information could be used for a commercial purpose. It's who gets to decide what that purpose is.

Right now, you have a situation where the act says the company decides what the purpose is, then it can decide whether or not you consent. I don't even know that information is being collected about me in a number of situations, and it's not just on the Internet.

I have two comments about the Internet, which go back to a comment you made, Mr. Wappel.

The Chair: I'll give you two seconds for that.

Ms. Valerie Steeves: Okay.

The Chair: Make it one comment.

Ms. Valerie Steeves: Okay. I went to Bell Canada and I bought a phone and my phone number somehow got into the hands of somebody who is sending me text messages. I get about 30 a day, and they're junk messages, but I pay $1.25 for the privilege every time I get one of these junk messages. I have no idea who has my information. I have no idea how they got it and I need some mechanism that allows me to go to a corporation and say I need to know this so I can make a decision about whether I want to get these messages or not.

PIPEDA will get us there as long as you have a chance to look at tightening up the language. Give it a shot. It will work.

The Chair: Okay, thank you.

Commissioner, I'll give you an opportunity to answer any of the four, particularly any comments on surveying children.

Mr. David Loukidelis: If I can address the—

The Chair: From B.C.

Mr. David Loukidelis: If I could address the question of cookies first, consistent with what I said earlier, I would not suggest that, again in the B.C. context, we take a technologically oriented approach to these things. I think general principles of privacy legislation should continue to be the order of the day. When it comes to cookies specifically, there are tools in your Internet browser, for example, and there are third-party pieces of software that you can often get for free on the Internet that will allow you to exercise an incredible degree of control over cookies. For exmple, you can choose to accept or reject cookies, as you see fit, and to allow yourself to be tracked as you surf across the Internet or not.

On the question of surveying children, clearly that introduces some very sensitive issues around the ability of youth to understand what it is they're entering into when they give up some of this information, sufficiently so that in the U.S., Congress passed the Children's Online Privacy Protection Act of 1998. Again, it is early days for these laws in Canada. For my part, I would hope that in British Columbia, we can, only three years into our law, continue to work with industry to try to ensure that in the case of children and generally in relation to some of these technological challenges, those general principles are adhered to and that the legislation works well in its present form without radically altering the approach to some of these technologies.

● (1615)

The Chair: Thank you.

Mr. Tilson.

Mr. David Tilson (Dufferin—Caledon, CPC): Thank you, Mr. Chairman.

Commissioner Loukidelis, I appreciated your comments about the "work product information". That has been discussed in the committee. You may be reluctant to get into this, but Commissioner Stoddart gave evidence to the committee that the national commission looks at each matter on a case-by-case basis, as opposed to a specific definition. I don't recall, but I don't think she really said that we should have a definition. Can you talk about that—the specific definition versus what the federal government is doing, looking at matters on a case-by-case basis?

Mr. David Loukidelis: Sure.

As I mentioned, in British Columbia's law we have a definition of "work product information", and clearly the legislature, using specific language, has given me direction. It's my obligation, on a case-by-case basis, if the matter actually comes to me in a formal inquiry, to interpret and apply those words as intended by the legislature.

Having said that, if we didn't have that definition, and if in fact we were to fall back on a definition of "personal information", which is "information about an identifiable individual", you would still have the same opening that has been taken here by my federal colleagues and in other provinces under their public sector legislation to try to interpret what information is "about" an individual in the sense intended by the legislature, and perhaps coming to the same result that has to be said.

Mr. David Tilson: Except, I suppose by not having a definition, case B could be quite different from case A, even though they're almost identical.

Mr. David Loukidelis: There would nonetheless be some play at the margins. It's the old struggle between specificity and generality in legislative drafting. I think, though, if you have a decision that clearly sets out the principles for interpreting what is meant by "information about an identifiable individual", you could come ultimately to the same result, subject to a different view being taken by the courts.

Mr. David Tilson: On the business transaction issue that you talked about, corporations or businesses selling their business to someone else, I'm just wondering how much the state should interfere in that. For most transactions or most sales of businesses, that non-competition clause and that non-disclosure clause are routine clauses in almost any of the agreements I've ever heard of. If people choose not to have that, is the state interfering too much in personal business transactions?

Mr. David Loukidelis: I would characterize the special provisions in British Columbia's law dealing with business transactions as enabling or facilitating business transactions, by relieving businesses primarily of the obligation that would otherwise apply, to go back in each instance of a sale of a business or a substantial portion of a business and get consent from individual consumers, employees, customers, shareholders, senior management, and so on. It in fact relieves them of the consent obligation and tries to appropriately facilitate change of control, sale of assets.

Mr. David Tilson: I'm just saying that's generally done anyway, as opposed to the state mandating it.

Mr. David Loukidelis: I think the concern would be, under British Columbia's PIPA, that you can't disclose personal information without the consent of the individual. Now, it's true that at the time—and this is going to the point you've made—you collected the information from your customer you could, in a notification to them, which is required under the legislation, say, and by the way, in addition to using this information in order to sell products or services to you, we may disclose it for the purposes of a business transaction, but I think some certainty was sought by the legislature, including that particular set of provisions.

Mr. David Tilson: On this business of a survey, Ms. Steeves, my only observation is that somewhere along the line we've got to take control of our own actions. My God, normally, with children in particular, when there are phone calls that come in and people ask what do mommy and daddy do, you train your children not to give that information out. In fact, normally you say don't take cookies from strange men who are walking along the street. Normally you say, with respect to whether it's on the Internet or whether it's on the phone, don't give out that information. In fact, you tell your spouse don't give out that information, because God knows where it's going to get out.

When you're out at a fall fair and you sign your name to a lucky draw that gives you something, there's always a price for that. Who knows where your name's going to get out?

And I guess it's the same question I'm asking to Mr. Loukidelis: somewhere along the line, can the state go too far in interfering in people's lives? It may mean that the whole process, which Commissioner Stoddart has talked about, and to a certain degree I'd agree with her, is the issue of education. There's a price to pay for giving out this information, as opposed to saying thou shalt not do it.

● (1620)

Ms. Valerie Steeves: The legislation is set up to use consent as a mechanism, to allow people to make those choices. One of the problems with this is that people often release the information in a social situation, not realizing that it has commercial consequences.

I do a lot of privacy education for a K-13 kind of age range. I've written a number of multimedia games designed to teach kids to protect their privacy in cyberspace, and in the real world, and all that type of thing. I cannot agree with you more about the importance of education and public discussion on these issues.

At the same time, I think we have to recognize that these kinds of invasive practices are being embedded into social environments where people don't realize that there is a cost to pay. When I was talking to my—

Mr. David Tilson: If I could interrupt, let's say you pass a law that says you can't do that, whether it's for children or adults or anything. How are you going to enforce that?

Ms. Valerie Steeves: I'm a bit bemused, because right now we have a law that says if you want to do it, ask, tell me, and then I can make a fair decision about it.

Mr. David Tilson: What if they don't? What if you have a guideline or a policy or a law that says you can't do surveys to children or whatever—to adults, for that matter? I have a lot of problems with saying people can't take surveys. If you don't want to do a survey, you don't participate. I'm asked to do surveys all the time. Most of the time I say I'm not going to do them.

Ms. Valerie Steeves: We do have a law, and the law says if you want the information, ask for it. And if somebody gets this information from my children then I have procedural rights under the data protection legislation, under PIPEDA, that I can enforce. So I can go to the Privacy Commissioner's office. I can lay a complaint. There can be an investigation. The practices can be looked at to make sure that they conform to that basic principle.

Mr. David Tilson: What should be the penalty?

Ms. Valerie Steeves: We have penalties under the legislation now.

Mr. David Tilson: I'm asking you, what should be the penalty if these are...? You've made a number of suggestions—

Ms. Valerie Steeves: Yes.

Mr. David Tilson: —that there are violations of getting information from people, and that perhaps the government—you haven't said it, but you've implied it—should take some sort of action to stop that from taking place, either getting their consent or doing something. What if they don't do it? What should be the penalty?

Ms. Valerie Steeves: That's what we've got. That's the status quo. That's what the law does under PIPEDA. It says if you didn't get consent to get that information, then the commissioner can order you to stop doing the practice. You can try to conciliate with the parties to come up with a solution that suits. That's all in place.

Mr. David Tilson: So there's a rule out that says that you—

The Chair: Sorry, we're way over time.

Round two, we'll have Monsieur Thibault, Mr. Stanton, Monsieur Laforest, Mr. Wallace, and then Mr. Van Kesteren. That's round two, five minutes each.

Welcome to the committee, Monsieur Thibault.

Hon. Robert Thibault (West Nova, Lib.): Merci.

Thank you both for appearing.

I understand your point about having this technology and a neutral type of approach, but there seems to be.... We talk about the Internet, but there are also cellphones and all these other technologies that are growing so quickly it's impossible to control. Even if you have all the companies, such as Microsoft and their move on pornography and all those things, there are still going to be ways to get around it. I think education on how to protect yourself becomes very important.

Just to make the point, I think we're going to have to consider the technology specifically, because it is going so fast. It's almost impossible to know when you're giving out the information. The consent mechanism isn't necessarily there. Sometimes they'll assume by the very fact that you are on that site that you are giving consent.

I went to the site of one of the large news organizations. I go there every day to check the price of oil on the commodities market. Before too long, I noticed I was getting unsolicited suggestions on stock picks. Included in that were some executable files. I delete everything, because I don't know what it is. I don't know if I ever gave consent for this. If I did, I didn't do it knowingly, but somehow it's there. There are a lot of difficulties with it.

I have a bit of a problem, generally, when we try to legislate these things, because these are from the consumer and commercial market. I don't like that my name and information is being sold because I bought a pair of headsets. They ask me for my phone number and these things in an electronic store. More and more you go there, and the first reaction is that you're filling in some personal information. Rather than just paying for your thing, they ask for this other information.

But there is the other side of it. There are things that I think are in the interest of society. The understanding of the laws and the application of the laws have become very difficult. I'll give the example of health care. It seems to me to be quite reasonable that when I go to a pharmacy he takes my social insurance number or some number and knows every drug that I've ever taken in my life—and that the doctor I visit has the same information. But not everybody agrees to that. Some information should be personal, and they don't want it floated out there. For the improvement of our health system, I'm willing to give up some privacy. I won't do it for commercial purposes.

To try to draft that regulation or that legislation in all provinces and all sectors and meet all those criteria becomes very difficult.

I wonder if you could comment on those points about the public interest and the individual's right to privacy.

● (1625)

Mr. David Loukidelis: Certainly.

Addressing the last point, about health care information and health privacy, there's a considerable investment now underway in creating pan-Canadian electronic health records. There is a challenge, of course, in ensuring that the privacy approaches in the various jurisdictions within Canada are brought into line.

There has been a considerable amount of work done. My federal colleague, Jennifer Stoddart, has worked with federal departments, for example, in creating an interpretive guide to PIPEDA in the health care setting. There's a federal-provincial-territorial harmonization framework on health privacy that is meant to promote harmonization so that the electronic health record initiative can move forward.

Difficult decisions are being taken across the country about the appropriate balance between the public interest in the sharing of personal information for health care delivery, to ensure innovation, research, and appropriate allocation of resources, and the private interest in one's health information. Where that balance lies I think is a dynamic balance, and not really my place to say.

I know in British Columbia certainly there are extensive discussions underway, and the government is being consulted on those. Among the issues being discussed is how technological tools can help individuals ensure that the most sensitive of their personal health information is directed only to those health care professionals who really need to know it for delivery of a particular service to that individual.

The Chair: Professor, do you have a comment?

Ms. Valerie Steeves: As you know, you have an interesting mix of federal and provincial jurisdiction here. PIPEDA captures health information that is traded through the course of a commercial activity. The argument is made that information needs to flow within the health care community to ensure Canadians get the benefit of appropriate health care and all those types of things. At the same time, I think it's important to recognize that this information has an incredible value in the marketplace—it's worth a lot of money—and it's used for other purposes as well.

For example, I was contacted by a Canadian doctor who was sitting in his office when he got a knock on the door and a drug rep walked into his office and began going through his prescription records. He said he had a list of every woman in the doctor's practice between the ages of 35 and 55, and asked why they weren't on his drug for hormone replacement therapy. There's evidence that pharmaceuticals spend tens of millions of dollars a year to profile doctors solely to sell product.

When we create these infrastructures that allow the flow of information for the public interest, I think we have to be cognizant of the fact that there are secondary purposes and there are unintended consequences for that. When health information in particular flows out of the confidentiality, gets outside of that relationship between the doctor and the patient, all the evidence that I've been able to dig up in the research indicates that people respond by lying and hiding and not going to the doctor.

It goes back actually to a comment of yours, Madam Lavallée, about the importance of privacy as a social value and a human right. Privacy is more than the control of our information. It's how we negotiate the relationship between ourselves and others. It's central to our ability to trust other people, to enter into social relationships. When we allow that information to flow, if we don't respect the social value of privacy and the importance that privacy plays in the democratic process, we're going to end up with these unintended consequences and we will have people hiding and not going to the doctor because they'll only go if they know what they say to the doctor is confidential.

I think it's interesting that PIPEDA captures health information because it underlines that this is a commodity that's traded in the marketplace that's worth a heck of a lot of money. We have to be particularly careful when we examine those kinds of arguments that it should flow for the public interest because those unintended consequences aren't necessarily going to get you where you think you're going to end up.

● (1630)

The Chair: Thank you.

Mr. Stanton.

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chair.

To our witnesses today, thank you very much for attending this afternoon.

To Commissioner Loukidelis, on the question of the degree of remedy or response that PIPEDA currently provides, I understand in the B.C. format you have the ability to make orders and to force compliance with issues, which perhaps isn't available within PIPEDA. I wonder if you could relate the B.C. experience and comment on how things have played out compared with the ombudsman approach that the current federal act provides.

Mr. David Loukidelis: Thank you for the question.

I'm happy to relate the B.C. experience as briefly as I can. It's the only experience we know in British Columbia, beginning in 1993, with the enactment of the Freedom of Information and Protection of Privacy Act, which is the provincial public sector access to information and to privacy protection legislation. It covers over 2,000 public bodies in British Columbia. We've had an order-making power, and that is also the case, as you've said, under the Personal Information Protection Act. Since the beginning of 2004, we've had an order-making power.

However, it has to be emphasized that it is by no means the tool of first choice for our office, speaking for myself or indeed looking at the experience of our office. Looking again at the public sector experience, we always refer complaints about privacy issues or access to information appeals—and we have order-making power in that respect as well—to mediation by one of my colleagues. And we settle something like 88% to 91% of all those matters by mediation.

That's the approach that we're taking under PIPA as well. We refer complaints to mediation. In the three years, just about, that PIPA has been in force, I've issued seven binding orders under PIPA. The remainder of the matters we have been able to deal with in a mediation type of approach, which is consistent with the approach taken, as I understand it, in every important respect, here in Ottawa by my federal colleague and in other commissioners' offices across the country.

We have other tools as well. For example, we can refer would-be complainants back to the organization in question, which we do in many cases, to try to resolve the matter first, as a private matter, if you will. We also can refer individuals to other appropriate processes—for example, the grievance and arbitration process, if there's a collective agreement in place—which we do quite regularly, or to the human rights process as well. We sometimes refer them to mediation by private sector organizations, for example, as such chambers of commerce. And we also use our powers to educate consumers and organizations, as we've done in the public sector, and to produce supportive resources for them, guidance, if you will, on interpretation and application in a very practical sense, at least as best we can, to implementation of legislation, to try proactively to avoid complaints arising in the first instance.

So there's a whole array of tools, and the order-making power is far from the first one we reach for. In fact, in many respects, you could say it's the last tool we reach for.

Mr. Bruce Stanton: To follow up on that to a degree, in the same light at the federal level, in a few instances the Privacy Commissioner has pursued the use of the Federal Court, which is the course of action available, but it's very much the minority of files. And they've used the investigations, the audit, the report approach to find and mediate these situations.

From your point of view, should we be looking much more closely at a great departure from this ombudsman model we currently have in place, based on your experience?

● (1635)

Mr. David Loukidelis: I'm obviously aware of my federal colleague's testimony on this issue to you earlier this week. It has worked well for us in British Columbia, given the nature of the organizations we deal with in the public sector, but also the nature of the organizations we deal with in the private sector. We have a much higher proportion of small and medium-sized enterprises in British Columbia than in the federal context, where you're dealing with banks, other large financial institutions that are federally regulated, such as telcos, where the ombudsman approach may have different benefits, if you will.

I agree with you that other tools are available to my federal colleague: recourse to the Federal Court, for example, and the audit power, which I understand she has started to use under PIPEDA, as well. So it's not as if the ombudsman approach is without sharper implements, if they're required.

Mr. Bruce Stanton: Thank you, Mr. Chair.

The Chair: Thank you, Mr. Stanton.

Monsieur Laforest.

[*Translation*]

Mr. Jean-Yves Laforest (Saint-Maurice—Champlain, BQ): Mr. Loukidelis, in B.C., you can make orders dealing with complaints. You said you had to make orders eight or nine times in the last few years.

Commissioner Stoddart said herself that it was not a priority in federal legislation, at least for her office, to ask for the power to make orders.

You talked to us about your own experience. You said you referred complaints to mediation and to someone else. Even if this is not included in legislation, doesn't the authority to make orders and find many kinds of other solutions reduce the number of complaints or at least improve the complaints review process?

[*English*]

Mr. David Loukidelis: It would be difficult to control whether or not you had the power. It's an impression. I can only offer you that. I don't think the fact that we have the power to make orders is likely to decrease the number of complaints we receive. In fact, I suppose you could argue the contrary: the fact that we can order an organization to stop doing something or to destroy personal information that it has inappropriately collected might encourage complainants to come forward.

Certainly almost all of the complaints we get, which vary in number from about 150 to 180 a year—the number is increasing, of course, as the legislation matures, and as people become more aware of it—we address through means less formal than reaching for the order-making power.

I suppose you could add that the possibility that an order would be made might concentrate the mind of the organization somewhat, but again there are other ways of ensuring compliance. Our experience has been that, generally speaking, organizations, once they're aware of their obligations under the legislation and once we discuss them with them, are more than willing to comply rather than having to go the formal route.

[*Translation*]

Mr. Jean-Yves Laforest: This is exactly what I meant in my question. Basically, when you say that we shouldn't lose this power since this would eventually increase the number of complaints, I can put this in perspective.

But at the federal level, the Commissioner said she didn't need this power for the time being. However, if she had it, complaints could possibly decrease or at least companies and businesses could be persuaded, as you just said, to comply which would diminish the number of complaints. Companies would be more careful in the management of personal information.

● (1640)

[*English*]

Mr. David Loukidelis: I understand that the experience here, generally speaking, is that there is good compliance on the part of federally regulated organizations. Again, perhaps as the legislation becomes better known, and there's more and more experience with it.... Even if we didn't have the order-making power in British Columbia, we certainly would be using the same array of tools that were available federally to try to ensure that the compliance was consistent, and then, in fact, it would increase as the experience with the legislation moved forward.

[*Translation*]

Mr. Jean-Yves Laforest: Thank you.

The Chair: Thank you, sir.

Madame Lavallée, there's one minute left.

Mrs. Carole Lavallée: I'll just take a few seconds to ask you a basic question about fundamental rights.

You're suggesting in one of your recommendations to make the protection of personal information a basic human right. Don't you think there are cases where some basic rights take precedence over others and that you should sometimes be able to get personal information from people against their own will?

I will very quickly give you an example concerning the Correctional Service of Canada. When officers of the Service are attacked by inmates and there is an exchange of bodily fluids, which is most of the time deliberate and vicious, the officers cannot access the inmates' personal medical files.

Do you find this acceptable?

[*English*]

Ms. Valerie Steeves: First of all, privacy is recognized in Canada as a fundamental human right in a number of ways. Canada is signatory to international documents that underscore its commitment to the protection of privacy as a human right. The Canadian charter has been interpreted to include protection against unreasonable search and seizure where you have a reasonable expectation of privacy.

The fact that privacy is a human right doesn't mean that as a society we don't need to balance that right against competing rights. Freedom of speech isn't absolute in Canada; there are criminal limitations on what you can say. Privacy isn't absolute in Canada as well. There are a number of occasions where the courts, in particular in the criminal context, seek to find the right balance, when you have these situations where you have competing interests at play.

My argument is, if you recognize privacy as a fundamental right in PIPEDA, that what you're going to avoid is balancing that fundamental right against commercial profit or convenience. We don't balance off the right to freedom of speech because somebody could make some money if it were repressed. We come to situations where we have to decide where the limits are, when we're balancing right against right.

In the example you pointed to, there is a body of case law that has been developed to deal with that delicate balance. And it is a delicate balance; it is a difficult balance.

The suggestion I'm making is really drawing on the Finestone report, when the standing committee did an extensive public consultation on the impact of new technologies on privacy rights across the country. The recommendations of the standing committee at the time were that data protection legislation was necessary for the private sector, but they argued that data protection legislation will only fully protect privacy because of all the things we've discussed. It is a complicated environment, where information is flowing in all sorts of different ways, and our relationships are changing because of the platforms we're building.

Data protection will only be implemented in a way that gets us to where we want to be as a society if there is some umbrella commitment, some umbrella piece of legislation that recognizes that privacy is a fundamental value; it is a democratic value, a social value, a human right.

The suggestion of the Finestone committee was to enact a privacy rights charter that simply made that a statement of principle.

The Chair: Let me stop you there, Professor, because there are other people who wish to ask some questions. Thank you.

Mr. Wallace.

Mr. Mike Wallace: Mr. Chair, I will try to be succinct. I am going to ask the commissioner some questions first.

One thing we've heard previously—and you can let me know whether British Columbia does it or not—is that if there is a breach.... I think our Liberal friend, who isn't here today, talked about a credit card: there has been an error, and people's private information has gone out, and there are hundreds and thousands of them, or whatever. Does the legislation in British Columbia require the company to notify the individuals that their information has been breached?

● (1645)

Mr. David Loukidelis: The short answer is no. The only legislation in Canada of which I'm aware that has that requirement is Ontario's Personal Health Information Protection Act.

In British Columbia—and our legislation is up for its own statutory review, starting in the next few months—I would, if asked, at this time certainly not support any explicit notification requirement along the lines of what we've been seeing in the United States, for example. I think that as the legislation matures we should wait for evidence that mandatory notification actually is a cost-effective way to reduce risks, for example, of identity theft flowing from a so-called data breach.

For now I would prefer strongly to continue with our office's approach to assessing this, looking at risk under the PIPEDA obligation of organizations to take reasonable security measures to protect personal information against unauthorized use; and to work with organizations and issue guidance, which we are about to do—and we have been joined in this in the last little while by our Ontario colleagues—around risk assessment as to whether or not notification would be prudent.

Mr. Mike Wallace: Okay. You took my second question. Thank you for answering it.

The third question I had for you, and I just want to be clear on this, is: even though there is different privacy legislation—provincial, or federal in the absence of provincial—if I had a business that worked nationally, including in Quebec, are you telling me that there is no real, significant cost to business in doing something in British Columbia that I have to do differently in Alberta, or in Quebec, or in P.E.I.?

Mr. David Loukidelis: I'm a lawyer by trade—

Mr. Mike Wallace: We won't hold that against you, actually.

Mr. David Loukidelis: —with the usual caveats. I'm sure I could find many others in the legal profession who might take issue with what I'm about to say, but I would suggest to you that the similarities among the laws across Canada far outweigh such minor differences as may exist, and an organization that ensures that it is securely in compliance with PIPEDA, for example, with particular regard probably to the legislation in Quebec, would be well placed to say to me, and to perhaps others, even—and my colleague in Alberta might not like it that I've said this—that we're fine with your legislation.

Mr. Mike Wallace: Okay.

Mr. David Loukidelis: There are nuances, so there will be some costs there to ensuring that you've ticked all the boxes, but it is not as onerous, as I said at the outset of my remarks, as some might suggest. I would suggest to you that in other jurisdictions—the United States, for example—the costs are much higher to try to comply.

Mr. Mike Wallace: Higher, okay.

On the employee privacy piece, you said there is no direct consent needed for people's employment information, the basic employment information. Does that include their salary? Is that basic employment information?

Mr. David Loukidelis: An organization, in principle, would be able to disclose one of its employees' salaries to a third party, the amount of the salary, but only if it was solely for a purpose reasonably required to, for example, maintain or terminate the employment relationship, and if that disclosure, that particular disclosure, was reasonable in the particular circumstances.

Mr. Mike Wallace: So in the case of an insurance company calling on another company, wanting to bid on, I don't know, some sort of product that they may be purchasing for their employees but is affected by the amount of payroll they have, it's not by individual, by a gross amount they're allowed to say that, but they're not allowed to give what each employee makes, is that an accurate—

Mr. David Loukidelis: I have two quick points in response.

If the information is aggregated payroll, it is almost certainly not information about an identifiable individual, so it's not caught as personal information. It is therefore not covered by PIPA.

Our PIPA also has a special set of rules around the collection, use, and disclosure of personal information for the purpose of enrolling somebody as a beneficiary in a benefit plan or for something like group life insurance.

Mr. Mike Wallace: So under your legislation, you can or cannot do it?

Mr. David Loukidelis: You can.

Mr. Mike Wallace: You can do it.

Mr. David Loukidelis: So even if it were personal information, consent is not required for the purposes of enrolment and maintenance of those plans.

Mr. Mike Wallace: Do I have any more time?

The Chair: No. Thank you, Mr. Wallace.

Commissioner, you mentioned the review. Section 59 of your act says that the review must begin within three years of January 1, 2004, which would mean, presumably, no later than next month. Usually these deadlines end up not meaning anything, but I'm wondering, in your preparation for your appearance before the special legislative committee of your province, are there any major issues under your act that you see coming forward that you're going to bring to the attention of the committee, that may in some way be interesting or relevant to this committee's review of PIPEDA?

● (1650)

Mr. David Loukidelis: The committee contemplated by section 59 has not yet been struck. We're in the process of getting our brief together for the committee for when it is struck and the review actually begins. But certainly to the extent that I can provide the committee here with information in the coming weeks and months that might be of use to you, I'd be happy to do that.

The Chair: Weeks would be better than months, as far as this review is concerned. Thank you very much for that.

We'll now go to Mr. Dhaliwal, followed by Mr. Van Kesteren.

Mr. Sukh Dhaliwal: Thanks, Mr. Chair.

My question is to the commissioner.

Earlier, Professor Steeves was talking about the doctor collecting information on hormone replacement therapy and then giving it to the pharmaceutical companies. The way I look at it, it helps society when it comes to research into hormones and is the only way that industry can find out where the need is and what the needs of the consumer or society are. As long as the personal names of those women or other patients is not disclosed to the pharmaceutical companies, would you consider that a work product?

Mr. David Loukidelis: Bearing in mind my initial lawyerly caveat around particular circumstances and general remarks, I think it's fair to say that the information you've described around the prescribing patterns of physicians, as opposed to patient information, on its face appears to fall certainly within the definition of “work product information” in the legislation in British Columbia.

Mr. Sukh Dhaliwal: You don't have any problem with that, though?

Mr. David Loukidelis: As a policy choice? It's not my place to make that kind of policy pronouncement, if you will, but I think clearly the legislature in B.C. has made that choice in defining "work product information" in the way it has because, as I say, on the face of it that kind of information—prescribing pattern information—would appear to fall within that definition and be within that policy decision.

Mr. Sukh Dhaliwal: Would you see us here considering similarly incorporating that into PIPEDA as well?

Mr. David Loukidelis: I don't know that I can usefully respond or make suggestions on that front. Clearly it's an issue that has been addressed through interpretation of the definition of "personal information" under PIPEDA—what is personal information about an individual. So whether or not it's necessary to add a definition in light of the fact that this interpretational approach has already been taken is something that I'll respectfully defer to the committee and others.

Mr. Sukh Dhaliwal: You are a politician.

The Chair: Ms. Steeves, there's been a lot of interest of committee members on the issue of work product. Would you like to comment on Mr. Dhaliwal's question?

Ms. Valerie Steeves: I'm curious as to whether or not you've had a chance to talk to organizations like the Ontario Medical Association or the Canadian—

The Chair: Not yet, but we will.

Ms. Valerie Steeves: Okay.

Often in the work I've done I've been told by GPs that they have serious concerns about capturing that type of information for two reasons. First, it can be de-identified but it's very difficult to make it truly anonymous, and they feel that puts their patient at some risk. Secondly, I've heard the argument made that this negatively impacts the relationship of confidentiality between the primary health care giver and the patient.

My last comment would be that I think we need to think more critically about the difference between research as a public interest or a public good and the commodification of this information for commercial purposes. PIPEDA already has exemptions for research for scholarly or statistical purposes, and that information is available, usually with consent, because most ethics committees are going to look for consent, and it does flow into the research community with certain ethical protections. You're talking a different thing when you're talking about selling the information in order to convince a doctor to give one particular pharmaceutical product rather than another that has the same medical indications.

● (1655)

The Chair: Okay, thank you.

Mr. Van Kesteren.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you, Mr. Chair.

Thank you for coming here.

I'm not a lawyer, but I understand that English common law all revolved around property rights. Are we in a new era? Should we be making laws that say thou shalt not, and if you do, bingo? Are we just dancing around this thing?

We know, for instance, it's against the law to be a peeping Tom, but if you change in front of the window and you draw a crowd, it's going to be a little.... So many of these things are... I want to go a little further. If I'm a small business, you scare the daylights out of us with all these laws, because really there's no malice there. I mean, a small business might want to have a customer list and maybe wants to make sure that this guy isn't stealing roses when he isn't paying for them. We're getting into areas where there seems to be a contradiction. On the one hand there are some things you're talking about, and we think, wow, we have to do something about this, but on the other hand, as Mr. Tilson said, if you're surfing the Internet and you're doing all the...like that peeping Tom, you're standing in front of an open window.

To get back to my first question, are we at a threshold where we have to develop a whole new set of laws?

Ms. Valerie Steeves: The point is that PIPEDA is the result of a negotiation between consumer groups and the private sector. They've worked out a bunch of rules that can work, and we've enacted them in legislation. I think we need to tighten those rules to make sure that we get the result we want.

Mr. Dave Van Kesteren: Yes, but we've made these rules that probably would deal with the areas you're concerned about, and I agree. Isn't there a whole host of people out there who really would never come in conflict with those things or never have any mal-intent?

Ms. Valerie Steeves: In response to your comments about small business, one of the things I've been privileged to work with the federal commissioner on is an educational module that's designed specifically for small-business purposes to make it easy and cost-effective for them to comply with the existing legislation.

Compliance has been seen to be quite a barrier, but I think that's because they haven't really rolled out that educational program yet. On small businesses, I agree with you, there's a lot of goodwill; they just want to know where the bar is, what hoop they need to jump through.

Right now there's confusion about the size of the hoop, and where it is, if it's over here and if it's over there. I think we need to give the educational mandate an opportunity to get out there and to create greater certainty for small businesses, and make it easier for small businesses to comply.

Mr. Dave Van Kesteren: So you're thinking we're in an evolutionary process, not necessarily that we need to look at this completely differently, and just say you can't do that. If there's new technology, you have to submit that technology. If something comes to the foreground that can be used where we need legislation, you don't think that's—?

Ms. Valerie Steeves: What I actually think is you as legislators will find that no matter what piece of legislation you're touching, you're going to tickle a privacy question. It's something that we need to raise in the public consciousness, but we also need to have an ongoing democratic debate between citizens and legislators. So there is a sensitivity to the importance of privacy as a social value, and it's not just through PIPEDA, it's through the Public Safety Act, it's through the Anti-terrorism Act, it's through a number of different pieces of legislation that will flow across your desks and you'll have to make decisions on.

Again, I go back to Madame Lavallée's comment. If we recognize the importance that privacy plays as a democratic value—it's one of the fundamental parts of the rule of law—if we recognize that, chances are that when we're making choices about all those other forms of legislation, we'll get the mix right.

So one of the opportunities that PIPEDA provides us with is the chance to look at the e-commerce environment to come up with rules that respect the fact that people should have some say over the flow of their personal information.

Mr. Dave Van Kesteren: Thank you.

The Chair: Thank you.

Members, do you have any further questions?

Okay, then I'll ask the last questions.

Since you're here, Commissioner, and we would appreciate your advice on this, since you are actively involved, I'll simply read the two questions and then you could address them.

Could you outline the circumstances in British Columbia that led to amendments to the Privacy Act to address concerns about the potential unauthorized disclosures of personal information to U.S. authorities pursuant to the Patriot Act?

Secondly, could you explain why amendments were made in this regard only to the B.C. public sector privacy law and not the private sector act?

● (1700)

Mr. David Loukidelis: Do you want the long answer or the longer answer?

The Chair: The medium-sized long answer.

Mr. David Loukidelis: All right.

The occasion for the concern is a number of complaints arose specifically around the decision by the provincial government to outsource to private sector service providers the delivery of certain public services, specifically the administration of the provincial health insurance plan, the medical services plan.

The result of our analysis was that there was a reasonable likelihood that certain orders or subpoenas under the U.S.A. Patriot Act and legislation that it amended could be issued to reach into Canada to get to personal information in the hands of the private sector service providers if they had a sufficient U.S. link.

The legislature, three weeks before that report was actually delivered with that conclusion, chose to amend the Freedom of Information and Protection of Privacy Act to make it even clearer that foreign court orders, foreign judicial process, could not reach extraterritorially into Canada with that effect, and to impose certain other requirements on public bodies in British Columbia around the protection of personal information of citizens.

No such amendments were made to the Personal Information Protection Act. And I have from the outset, as it happens, drawn a distinction between the public sector situation, where citizens are not in a position to consent or not to consent to the decision by government to outsource the delivery of public services involving their personal health information, and the situation in the private sector, where, certainly in principle and I think realistically in practice, individuals can vote with their feet. If they're not content with the personal information practices of a particular business, they can take their business elsewhere and make that consumer choice. I think that is a real and meaningful and substantial distinction that justifies the different treatment across the public sector and private sector divide.

The Chair: Thank you very much.

I want to thank both of our witnesses for very interesting and I think useful testimony—no question about it. I'm going to certainly be watching what I look at when I go to the store for Christmas shopping.

Have a safe journey back home. Thank you very much.

The committee is adjourned. We'll see you on Monday.

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca
