



House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 017 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Monday, November 20, 2006

—
Chair

Mr. Tom Wappel

Also available on the Parliament of Canada Web Site at the following address:

<http://www.parl.gc.ca>

Standing Committee on Access to Information, Privacy and Ethics

Monday, November 20, 2006

• (1535)

[English]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): I'd like to call the meeting to order. We have a quorum for the hearing of evidence.

Pursuant to the order of reference of Tuesday, April 25, 2006, and section 29 of the Personal Information Protection and Electronic Documents Act, we're undertaking a statutory review of the act.

I want to remind committee members that section 29 contains two subsections. The first subsection states that a committee of the House will review the administration of the first part. The second subsection states that a committee will undertake a review of the provisions and operation of the first part, and provide a report to Parliament that includes a statement of any changes to part 1 or its administration that the committee recommends. So the section provides for a broad-ranging examination of part 1.

I hope the witnesses today will be able to address the historical rationale for our reviewing part 1 but no other parts of the bill.

That said, I don't want us to keep repeating the long form of the bill, so I'd like to get us all saying "PIPEDA" the same way. I've heard people say "PIPEDA" and I've heard people say "PIPEDA". I'm going to ask the members of the department to give us some guidance, and then maybe the committee will be able to agree to pronounce it one way. We'll then encourage all other witnesses to pronounce it the same way, and no one will have to refer to the long form of the act from here on in.

With that little opening remark, allow me to welcome our witnesses today.

From the Department of Industry we have Michael M. Binder, assistant deputy minister, spectrum, information technologies and telecommunications; Richard Simpson, director general, electronic commerce; Danièle Chatelois, privacy policy analyst, e-commerce policy directorate, electronic commerce; and Alexia Taschereau, senior counsel.

Welcome to all the witnesses.

Mr. Binder, I believe you're going to make some opening remarks. Please, the floor is yours.

[Translation]

Mr. Michael Binder (Assistant Deputy Minister, Spectrum, Information Technologies and Telecommunications, Department of Industry): Thank you, Mr. Chairman. I'm delighted to be here today to discuss this legislation with you.

[English]

You've already asked me probably the afternoon's toughest question. The answer is that we call the bill "PIPEDA", but I too have heard all kinds of variations. Whether or not you want to adopt our pronunciation is up to you.

You may wonder why Industry Canada is responsible for this particular piece of legislation. Let me tell you that we started worrying about the digital economy long ago. We anticipated the creation of databases and electronic commerce, the whole digital economy that goes with the Internet. We thought there should be pretty reasonable and clear rules of engagement in the marketplace in the so-called digital economy, particularly online. That's why we introduced this bill way back, after many years of trying to get consensus on what the provisions of this particular legislation might be.

As you know, a lot of people on the outside are very eager to appear in front of you to share with you their advice on how this legislation has been performing, and perhaps to give you their suggestions for improvement; you can always improve things.

With your permission, then, I would like to have Richard Simpson take you through a slide deck. I believe you all have copies of this particular deck. It tries to lay out what this act is about and the provisions in it. After that, maybe we can open up the discussion.

The Chair: At 22 pages, is it really a "slight" deck?

Mr. Michael Binder: A lot of it is to take away and read. We will go very quickly through it.

The Chair: Oh, you don't need to go very quickly. It's been five years, and we've been mandated to study the bill. We know there's great interest in it. We're not trying to rush you by any means, but we want to leave time for questions and for engagement with the committee members.

And I notice the deck is on thick paper, so it really isn't that thick.

Please do go ahead.

Mr. Michael Binder: Richard.

[Translation]

Mr. Richard Simpson (Director General, Electronic Commerce, Department of Industry): Thank you and good afternoon.

You have received copies of the document that we will refer to as we provide an overview of the legislation.

[English]

I'll go through the individual slides, as you've suggested, Mr. Chairman, quite briskly. Please stop me if you want to ask a question at a particular point.

If you look at the first slide, which shows in graphic format the size of the online marketplace in Canada, the key point is that the protection of personal information is a core element in the legal framework for a global networked economy.

The next slide gives you a brief chronology of work that has been under way for a number of years on privacy protection, both here in Canada and internationally. Some of the key dates are 1984, when the Organisation for Economic Co-operation and Development, the OECD, issued guidelines for the protection of privacy and transborder data flows. This is quite important, because it has formed the base for privacy protection laws in several jurisdictions, including Canada and many European countries in the European Union.

The second date, 1996, the CSA Model Code for the Protection of Personal Information was released. You'll see in a moment that this is a core component of Canada's national legislation on privacy and the privacy regime in Canada generally.

The other dates really take you through the phased implementation of PIPEDA. It initially came into force in January 2001. It was extended to the health sector in 2002, but only came into full force in January 2004.

• (1540)

PIPEDA has two main parts, as slide 4 points out and as you've already pointed out, Mr. Chairman. The first provides the privacy protection obligations under the act. Parts 2 to 5 comprise the section dealing with electronic documents, and this part has a number of provisions that enable more effective use of electronic technologies within the federal government administration. It amends the Canada Evidence Act, the Statutory Instruments Act, and other legislation, and has a number of provisions that allow government departments to make use of e-business and electronic commerce techniques in their day-to-day administration.

Part 1, for privacy, actually sets the rules for the private sector in protecting personal information. If you look at the summary statement of the purpose of part 1 on slide 5, you can see that part 1 establishes these ground rules governing "the collection, use and disclosure of personal information". You'll hear those words used quite often. The different rules regarding collection, use, and disclosure of personal information are set out quite clearly in the act.

The act balances two central considerations that are also contained in that statement of purpose: the need to protect the privacy of individuals and the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would

consider appropriate in the circumstances. This really reflects the business reality that personal information is routinely used by consumers, businesses, and other organizations to conduct trade and commerce, and even more so in an online world.

On slide 6 we have tried to outline for you the key features of PIPEDA. First, it applies only to personal information and only to personal information that's used for commercial purposes. This is quite important in terms of defining the area and scope of the legislation.

Second, a very important feature is that this is built on a private sector code. It's a self-regulatory initiative, as it were, taken from the Canadian Standards Association. It's built on the CSA Model Code for the Protection of Personal Information, which, as I mentioned, was adopted before the legislation came into force. It's technology-neutral, although it certainly relates a lot to the way in which electronic technologies are now using and manipulating personal information and data generally. It applies to personal information in all formats, electronic and non-electronic. It applies across the economy as a whole; therefore, it has a broad marketplace scope and does not apply just to individual sectors. It's not based on criminal law and enforcement, but is enforced through the Privacy Commissioner of Canada and the Federal Court.

There are other key features. Just as important is what PIPEDA does not apply to. It does not apply to non-commercial activities or to non-personal information. There's a lot of data out there in electronic and non-electronic form that is not personal information and is not captured by the legislation. It doesn't cover any government institution that is subject to the federal Privacy Act. That's a different act; it is within the scope of this committee's interest, I know, but it is separate from the rules in PIPEDA. It does not cover employee records in the provincially regulated private sector. And there are a number of other areas that are not captured by the legislation.

The essential requirements and obligations under the act, as slide 8 points out, are cited in sections 3 to 5 in the law, but the real obligations are laid out in schedule 1, which, as I mentioned, is the CSA Model Code for the Protection of Personal Information. Subsection 5(3) has a further qualification about the need for a reasonable purpose test. You'll hear about that from many people.

The model code, schedule 1 of the act, has 10 basic principles. I won't go through all the details of those for you, but I think probably first among equals on that list is the need for consent. All privacy legislation, not just in Canada but in many other countries, is founded on the principle of consent.

•(1545)

There's also a number of principles—purpose, limiting collection, limiting use—which really points to the need to define purpose and limit the use of personal information when it is collected. That is sort of a matching set to the requirement for consent.

There's a number of provisions relating to access to ensure the reliability and accuracy of information that is maintained on a person.

Mr. Michael Binder: If I may interject, Mr. Chair, it took about 10 years to get consensus of all parties—private sector, consumers, government—to come up with these ten commandments of privacy. I have to tell you this is the core understanding of the big policy issues that are embedded in this particular act.

Mr. Richard Simpson: Slide 9 points out that the act contains a number of exemptions relating to the consent requirement, which is contained in section 7, and also to the individual's right to access personal information, which is contained in section 9, and the bullet points out what those exceptions are.

The responsibilities and powers of the Privacy Commissioner, outlined in slide 10, are consistent with the role of ombudsman that the legislation assigns to the Privacy Commissioner. The Privacy Commissioner does not have the authority to make binding orders. She investigates complaints that are received or acts on her own initiative. She has a number of other powers, including an audit power. She publishes an annual report that comes to Parliament, as you know, since she is an officer of Parliament, and she has a number of responsibilities for both promoting the act, privacy protection, and educating the public. How the Privacy Commissioner's responsibilities are undertaken is a very important element of the legislation.

Slide 11 points out that the Federal Court acts as a backstop to the Privacy Commissioner with a number of responsibilities, eventually including the need to deal with an appeal by a complainant or the Privacy Commissioner on a particular finding. It also has some other powers, as you go to slide 12. As issues are taken before the Federal Court, there are some powers that the court can use to take action against organizations in violation of the act. But you can see that the number of points here make it clear that this is aimed at intentional and deliberate behaviour in violation of the law, such things as obstructing a commissioner in an audit or an investigation, rather than a regular exercise of power by the court.

In slide 13, PIPEDA also sets out—

The Chair: Pardon me for interrupting.

Back to slide 12, “the following are offences under PIPEDA”, section 28. You have a bullet point “taking action against an employee who is a whistle-blower.” These little bullet points and big bullet points are your breakdown of what the offences are. Is that right?

Mr. Richard Simpson: That's correct; they're offences that are specifically contained in the act on which the court can take action.

•(1550)

The Chair: Thank you.

Mr. Richard Simpson: Slide 13 sets out responsibilities for the Governor in Council. Some of these are very important to the functioning of the act. One of these powers is to make regulations to specify investigative bodies. A number of steps have been taken over the last few years to recognize private sector organizations that, by virtue of their responsibilities in legislation or in law, have to investigate and therefore have to both collect and disclose personal information

A second regulation power is to specify or define publicly available information. These are measures we can talk about in more detail. They're all contained in the regulations that have been distributed to the committee. You can find in there the operating definitions of publicly available information as well as all our investigative bodies' regulations.

The Governor in Council may also, by order, bind agents of the Crown to the act. This was really just a housekeeping measure, Mr. Chairman, in 1998 to ensure that certain crown corporations that were not subject to the Privacy Act would be subject to PIPEDA. This was to make sure there weren't gaps in federal crown corporations' being governed by privacy rules in one domain or the other.

The second power is to exempt from the act organizations that are deemed to be subject to substantially similar provincial privacy rules. The policy published in the *Canada Gazette* in August 2002 on that is also contained in your documentation, I believe.

Substantially similar, as we go to slide 14—and this may be worth focusing on for a moment—was a means Parliament put in place for aligning federal and provincial privacy laws around a single set of ground rules for data protection. Those rules would be the CSA model code, and they would apply across the economy as a whole.

In paragraph 26(2)(b), you see a power whereby the Governor in Council can exempt organizations that are subject to provincial laws considered “substantially similar”. In this case, the provincial regime for privacy protection would apply within that province, rather than the federal law.

The established criteria for “substantially similar” were to incorporate the CSA model code—those 10 principles—to provide for independent and effective oversight, and to restrict the collection, use, and disclosure of personal information to purposes that are appropriate or legitimate.

You'll see on the bottom of the slide that four provinces now have substantially similar provincial laws in place, and therefore those provinces have exemptions from PIPEDA: Quebec in 2003; the provinces of Alberta and British Columbia in 2004; and Ontario, in respect to their Health Information Protection Act, in 2005. So four laws have been recognized as substantially similar.

Essentially what this does is accommodate provinces that choose to legislate in respect to privacy protection, while allowing the federal law to apply in those provinces that choose not to do so.

As I mentioned, the Quebec privacy law was recognized as substantially similar in 2003. The Province of Quebec, however, has given notice of a constitutional challenge to part 1 of PIPEDA, which has to do with the clarification of the federal trade and commerce power in relation to provincial jurisdiction over property and civil rights. Although some documents have been filed, Mr. Chairman, the court still has not heard the constitutional reference. We expect that will occur sometime later in 2007.

The Chair: Mr. Simpson, is anybody going to comment on that? That's three years. That's a long time for a reference not to have been decided.

Mr. Richard Simpson: That's correct.

There have been documents filed. The court asked for affidavits to be filed by...I forget what the original date was. Initially the federal affidavit was filed in early 2005, I believe. Or was it earlier? Yes, it was in March 2005. That was then followed by a request for an affidavit from the Government of Quebec, which filed its affidavit in July 2006, and we have filed an affidavit in 2006.

You're right to think about the amount of time that has transpired since the original reference. I think that's partly because essentially it's business as usual in the province of Quebec, since their act has been recognized as substantially similar. The provincial privacy commissioner does exercise authority as beforehand within the province. It has been mainly the time it has taken for some of the litigants to put the material together.

• (1555)

Mr. Michael Binder: Yes, and we're informed, Mr. Chair, that they've asked for another extension.

Mr. Richard Simpson: That's correct.

The Chair: Who is "they", Mr. Binder?

Mr. Michael Binder: The Quebec government.

Mr. Richard Simpson: The Department of Justice.

Mr. Michael Binder: The Department of Justice.

The Chair: Is the federal brief all done?

Mr. Richard Simpson: Yes, it is.

The Chair: So it's not delayed on behalf of the federal government.

Mr. Michael Binder: No.

The Chair: All right, thank you.

Mr. Richard Simpson: We can make our affidavit available to the committee, if you wish. It's quite a good read, I have to say, in terms of the history of privacy legislation in Canada.

In the next slide, slide 16—

The Chair: I'm sorry, Mr. Simpson. Again, forgive me. You were just in the middle of slide 15, and at the bullet point you say, the decision "will confirm the federal government's ability to exercise its powers over trade and commerce". Don't you mean that the federal government hopes that the decision will confirm...?

Mr. Richard Simpson: Really, we meant the word in the sense of clarify the federal government's power in respect to trade and commerce in relation to provincial jurisdiction over property and civil rights.

The Chair: If the Quebec government were to disagree with the federal government's affidavit, the whole basis upon which PIPEDA has been designed, based on your second slide, goes down the toilet.

Mr. Richard Simpson: That's correct.

Slide 16 points out, and the committee should be aware, that there have been several modifications to the original law that have occurred since 2001. They're outlined there. Most of these respond to public safety requirements post 9/11, but there is also one revision that relates to the Public Servants Disclosure Protection Act, which will be amended by the Federal Accountability Act, which is now before Parliament, as you know.

That takes us to the parliamentary review itself, and if it's helpful, Mr. Chairman, we can share with you and the other committee members some of what we heard during informal consultations that we conducted over the last couple of years as the date for the review approached. These are outlined very briefly in the next couple of slides.

Overall, the consultations we undertook confirm that the privacy community basically believes that the act is working quite well. You'll see two quotes there that we picked up during our consultations, from the Information Technology Association of Canada and the Canadian Bankers Association, that confirm that.

Some minor amendments were suggested during those consultations, and some issues have been drawn to our attention relating to the state of privacy in Canada, not just to PIPEDA in the strict sense. The capsule summary of those comments is in slide 20, followed by slide 21.

The Chair: Mr. Simpson, again, forgive me. Just so that the record is clear, you said—our researcher just whispered in my ear—that the privacy community believes it's working well. Did you mean the privacy community or did you mean the business community, or did you mean both?

Mr. Richard Simpson: No, we do mean both. Certainly there's very strong support from the business community. As we get to talk about the powers of the Privacy Commissioner, you'll see that in the privacy community, generally speaking, the business community is very supportive of the existing role of the Privacy Commissioner, and you will hear from other members of the privacy community that even though the act is a good basis for protecting privacy in Canada, they have advocated some stronger powers for the Privacy Commissioner. You will hear that discussion, I think, as you call more witnesses.

● (1600)

Mr. Michael Binder: Most of the input was about improving the act rather than saying what is not working, but there are different opinions as to what the input might look like.

Mr. Richard Simpson: Absolutely.

As I mentioned, if you go to slide 20, one of the key issues is the role and powers of the Privacy Commissioner. You will hear from the commissioner herself quite soon, and she will certainly talk about that.

Another issue that has been brought to our attention will be called transporter data flows by some people. It's really the international dimension to the protection of privacy and the need to look at issues surrounding the increasing outsourcing and offshoring of data processing and therefore personal information. But there are a number of technical and definitional issues that have been brought up. The Canadian Bar Association has made a number of suggestions along those lines.

Looking at slide 21, continuing with some of the areas that will come to your attention that we have heard about, the employee-employer relationship and personal information having a different dynamic in an employer-employee relationship than it does in the commercial marketplace is certainly one issue that will be raised. There have been calls to remove privacy protection for employee e-mail and fax numbers, and this goes to the definition of personal information and whether or not it's like a telephone number and you need to protect employee e-mail numbers. Isn't it contact information, much as a telephone number is?

As for mergers and acquisitions, you'll certainly hear from witnesses regarding the need for flexibility in terms of due diligence relating to mergers and acquisitions. Again, you'll probably hear different views on that.

There'll be many suggestions regarding the definition of work product as something distinct from personal information. This is a technical issue that does have some significance in a number of sectors of the economy, and we can talk about that if committee members wish.

These are very likely the issues on which you'll hear a lot more from others, starting with the Privacy Commissioner, who has views on some of these issues. As the final word, the bottom line so to speak, the last slide points out some of the commendations or testimonials on the privacy regime in Canada that have received very high grades internationally from the business community, as you'll see in those quotations. Some of you may have seen *The Globe and Mail* article about two or three weeks ago that reported on a study

by Privacy International, which is an international group advocating stronger privacy protection across a number of countries. It ranks Canada and Germany with the best grades for privacy protection in the 30-plus countries they examined. So we do have a good basis on which to work, in our opinion.

Thank you.

The Chair: Thank you very much.

Just for committee members' information, I noticed the last quotation on page 22 is by Ray Protti. Many of you haven't been around as long as I have, but for your information, Ray Protti used to be the head of CSIS. If anybody would know what privacy information is good, it would be the former head of CSIS.

We are reviewing this, and before I go to questions, I'm going to ask the department this. You have had five years of talks with stakeholders. You have mentioned some of the issues that have come up. However, you haven't given us any indication of what the department's opinion is as the department in charge of this act in terms of those issues, and whether you particularly, as a department, have any recommendations for our committee. We don't necessarily have to take them, but naturally we would be interested if you do have some recommendations, particularly since you've been dealing with this act for five years with the stakeholders. I don't know if you're ready to tell us about that or if you've even thought about that, but I'd certainly invite you to think about it. If there are areas of the act you are in agreement with stakeholders and suggesters on, it would be appropriate if you told us that the department believes that X, Y, and Z is a reasonable approach based on five years of experience or whatever reasons you have, and that way, we could consider those items as we go through.

Has any thought been given to that?

● (1605)

Mr. Michael Binder: Let me say it this way. Five years sounds like a lot of time, but I have to tell you the actual law experience is only very recent. It took a long time to operationalize, for example, what is consent, how do you get consent, etc. The health sector didn't come on board until 2004. So it's only one and a half years, and that was a big carve-out.

Last but not least, that's not the way we normally operate. What we look for in this committee is to do this public consultation and provide advice to us, where then we'll take this through our internal processes, and if there is going to be any amendment following up, it has to go through our internal processes, go up to cabinet and legislation.

So I'm not trying to duck the question. I'm just trying to look for your guidance and advice after a formal hearing of inputs into our processes.

The Chair: All right.

I think my point was that if somebody had come to you and said X, and you fully agree with it and you think it would make sense for the committee to recommend an amendment to that regard, it would make sense to me that you would put that forward. I urge you to consider that. We may have you back later on, after we've heard from some of the witnesses.

We'll start with Mr. Dhaliwal.

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

Thank you, panel, for coming out and giving us a talk on PIPEDA.

You say there are four programs here that already have similar legislation in place, so this does not apply to them, right?

Mr. Richard Simpson: It does not apply with respect to the collection, use, and disclosure of personal information within those provinces. So the cross-border aspect of data protection still remains within the federal purview. So for example, the Privacy Commissioner in British Columbia has full authority to investigate complaints there and exercise all of his powers in relation to any privacy issues within the province of British Columbia. If it was a complaint about a collection of personal information from a B.C. resident, but it had taken place by an organization in another province, then that would go to the federal Privacy Commissioner and she would exercise her authority.

I should mention that there's very close cooperation between the privacy commissioners across the country. All four privacy commissioners in Ontario, Quebec, B.C., and Alberta, but particularly the three that have comprehensive privacy protection laws, collaborate very closely on an operational level with the federal Privacy Commissioner. She will tell you more about how that works. But that's one of the ways in which they ensure that there are no gaps between their respective jurisdictions.

Mr. Michael Binder: Mr. Chair, if I may, our original intention was to make sure that the business community doesn't have a patch of different rules across provinces. Business is more and more becoming national and international. In fact, we did emphasize that nowadays if you want to do business in Europe you have to have a piece of legislation that's acceptable to Europeans about protecting personal information. In fact, they went through our bill and they actually deemed it to be acceptable. So you can do cross-sharing of databases and information. They are quite happy with our legislation as is.

The same thing goes within a province. We didn't want one business to have onerous requirements in one province that are different from those in another province. That's why we established this national minimum standard, those 10 code provisions to try to put a national standard without imposing the specific on individual provinces in terms of the way they manage their own privacy issues.

● (1610)

Mr. Sukh Dhaliwal: When we look at today's emerging markets, today's emerging globalization, is the data that we collect also used for research purposes, or is it totally used for commercial activity? From your perspective, how much is it used in the commercial activities and how much is it used in the research activities?

Mr. Michael Binder: There's a two-key system here. It has to be personal and it has to be commercial for this act to apply. If it's not commercial, then the act does not apply.

Mr. Sukh Dhaliwal: So that means it has to have both personal and commercial together. Or can it be either one?

Mr. Michael Binder: Right. Both.

Mr. Sukh Dhaliwal: You said the latest group to come under this act is the health sector, right? You have the work product there. Could you go to the bottom of page 21 and elaborate on the work product and how it plays into this?

Mr. Michael Binder: There was a big debate. We use the example of whether a physician's prescribing patterns are private information for the physician or if they're private for the patients? There's a big debate about that, and presumably the court will determine what the outcome is.

Mr. Sukh Dhaliwal: Where do you stand on this, if you take this particular issue? If we look at the health community now, they are collecting the data. That's why I want it to come down to this particular issue here. On one side, it is the agencies that collect the personal information. On the other hand, it is the research and commercial activities based on those data structures that we have. And a third aspect is the physicians. By how much do they differ on this one, from all three perspectives—research, the agencies, and the physicians and their patients?

Mr. Richard Simpson: To go back, the premise for the legislation is based on the idea that it has to be personal information and it has to be commercial. There are a number of exceptions. Information that's collected for journalistic and artistic purposes, for example, is not captured by the act. It's exempt from the act. There are also a number of exemptions for particular types of research activity, even though scholarly activity is exempt from the act as well, correct?

There's a much broader definition of research for most people. Some research may be commercial. For that purpose, there are certain exceptions in the act for what I'll call commercial research purposes.

To get back to work product, I think you're right, it's a central issue around some questions in the health sector about the extent to which personal information is either protected individual information or work product information. You'll hear from witnesses that some provinces have looked at defining work product in such a way that it takes it out of the domain of personal information.

With respect to PIPEDA, a series of court judgments have defined personal information in such a way that certain types of data—like prescription information, if I'm correct—have been defined as not being personal information. In the federal law, we have not yet defined work product so that this area was exempt from the definition of personal information. Some provinces have. You will hear from some witnesses that there is merit in that approach. Others may have a different view.

So that's one approach. In terms of PIPEDA, essentially we in the health sector, at least, have gotten to a similar position due to court interpretations of the law.

I don't know if any of my colleagues want to elaborate, but that's how I see it working right now.

• (1615)

Mr. Michael Binder: I'm also told that the Privacy Commissioner deemed work product like this not to be personal.

We also have a carve-out for purely research data; that is, for pure research that is not in the commercial domain. Again, the act doesn't apply to it.

The Chair: Do I understand correctly that for work product like physicians' prescribing patterns, the Privacy Commissioner has ruled that not to be personal information? Is that what you just said?

Mr. Richard Simpson: Yes, the Privacy Commissioner reinforced that.

The Chair: Does the department agree with that?

Mr. Michael Binder: We have no difficulty with that. It's the law.

The Chair: There's a difference between having no difficulty with it and agreeing with it.

Mr. Michael Binder: Again, I'm going to sound like I'm trying to duck the question, but what I'm trying to say is that we are looking for advice on some of these issues. They are difficult issues. There is not necessarily a consensus on how they should be treated, and as you'll find out, there will be a difference of opinion about them. Therefore, at the end of the day, we will look for your advice and take this under your advisement.

Mr. Richard Simpson: Mr. Chair, just to add thirty seconds to the point, it is part of how PIPEDA works. The definition of personal information was left broad by Parliament, giving the Privacy Commissioner the opportunity to make some of these definitional interpretations in the context of his or her work. That's how it has unfolded. So it is important to know that the act is built around flexibility in terms of how the Privacy Commissioner defines personal information.

The Chair: Thank you.

Are there any questions from the Bloc? Madam Lavallée?

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Yes, of course. First of all, I'd like some information because there are several things I don't understand. I must admit that I'm new to the committee.

What exactly do you mean by personal information for artistic purposes?

Ms. Alexia Taschereau (Senior Counsel, Industry Canada, Department of Justice): In some cases, that could refer to lists of names and addresses for Christmas cards or invitations.

Mrs. Carole Lavallée: Invitations to exhibits, for example?

Ms. Alexia Taschereau: Exactly.

Mrs. Carole Lavallée: What exactly do you mean by "work product"?

Ms. Alexia Taschereau: I can give you an example as provided by the courts, namely prescriptions written by physicians.

Mrs. Carole Lavallée: So then, a work product could be a prescription or a report, for example.

Ms. Alexia Taschereau: Yes.

Mrs. Carole Lavallée: Aside from prescriptions, what else might fall into this category?

Ms. Alexia Taschereau: A report written by a person or employee as part of his work is considered a product.

Mrs. Carole Lavallée: I see.

I'm surprised that you've examined the whole question of prescriptions, since the health care field normally comes under provincial jurisdiction, or under Quebec jurisdiction. I don't understand why you've looked into this. Perhaps I'm missing something.

Ms. Alexia Taschereau: We mentioned prescriptions because they were identified by the courts as a work product. That example comes to mind. It's one area in which jurisdiction is shared. The act covers personal information regarding the health sector.

Mrs. Carole Lavallée: Yes, but nevertheless, the health sector comes under Quebec and provincial jurisdiction. You state somewhere that areas under provincial jurisdiction are excluded. Therefore, I don't understand you concern about prescriptions.

Mr. Michael Binder: When data is forwarded to another hospital, for example, a hospital in Ontario—

Mrs. Carole Lavallée: In another province.

Mr. Michael Binder: That's right.

Mrs. Carole Lavallée: Now that you've enlightened me, I have a question about the international implications of this legislation. You mentioned an organization called Privacy International which, if I understood you correctly, did a study of all international personal information protection legislation. You mentioned that this organization had reviewed legislation in 30 countries.

Have you contacted other countries with legislation similar to ours? Have you drawn comparisons? Can you tell us which important areas are covered by our legislation and which are not? What about other countries? You mentioned Canada and Germany, but I didn't quite understand if we were in the top percentile, as we say in Quebec when referring to education. Does our legislation compare well to that of other countries? What improvements would be warranted?

• (1620)

Mr. Richard Simpson: We have an agreement with the Europeans. An international standard has been set based on OECD-approved guidelines. This standard provides us with a level of privacy protection comparable to that of European countries.

I'm not familiar with all of the studies that have been carried out, such as the one done by Privacy International. According to that study, we currently measure up very well to other countries.

Mrs. Carole Lavallée: We rank in the top percentile.

In the comparative studies that you have seen - perhaps you haven't done one yourself — did you identify areas in which some improvements could be made?

Mr. Richard Simpson: Not really, because the standards that we have adopted are based on the CSA Model Code and they are the same as the ones adopted by European countries. We are almost at the same level.

Mrs. Carole Lavallée: Nevertheless, are there any components that could be improved upon?

Mr. Michael Binder: Comparisons are always being drawn between ourselves, the Europeans and the Americans. The latter take a different approach to privacy protection. They have passed legislation for each sector, whether the financial sector or the health sector. Their approach is completely different. We feel that ours is the best method, because the economy as a whole is treated the same way. It's interesting, because Mr. Gates, for example—

Mrs. Carole Lavallée: Are you talking about Bill Gates?

Mr. Michael Binder: Yes. The time has come for the United States to adopt an approach similar to ours, that is to pass legislation that applies to all sectors of the economy.

Mrs. Carole Lavallée: I see. Thank you very much.

[English]

The Chair: Mr. Martin.

Mr. Pat Martin (Winnipeg Centre, NDP): Thank you, Mr. Chair.

Thank you, witnesses.

I've been looking over the excellent research done by Nancy Holmes, our research staff member. I wasn't going to ask any questions, but I became alarmed about some things later on in her

research paper, at some of the things that she has recommended we ask you for your input on.

One is dealing with the duty to notify people in the event of a breach, especially in light of high-profile privacy breaches in data companies in the United States, etc. State laws are being enacted now such that in the event of a breach, there would be an obligation to inform the person that their personal information has been compromised in this way. This is interesting to me, because somebody came to me recently and said that Visa has three million breaches per year in Canada alone, and they don't inform Visa card clients that their personal information has been compromised. This is an alarming thing.

Would you recommend, in this first statutory review, that PIPEDA be amended to require that kind of duty to notify individuals in the event of a breach?

• (1625)

Mr. Michael Binder: If I may, we've heard a lot about that particular topic. There are those who are absolutely recommending strongly—and you will hear them in front of you—that the Privacy Commissioner name names. They may also make the suggestion to amend this legislation to force the disclosure of breaches of privacy.

Mr. Pat Martin: Not just the organizations that breach privacy; for instance, if it is Visa, then Visa would be obliged to tell me, if my card had been compromised, even if they fixed it and it didn't cost me anything.

Are we talking about the same thing?

Mr. Michael Binder: That's correct. That's the recommendation you'll hear a lot about. In fact, I think the Privacy Commissioner will be here, so you can ask her. She is deemed to have no power right now in the legislation to actually name names, so to speak, and to force the particular issue. This would probably require a legislative amendment.

The Chair: Not to take any time away from you, sir, but Mr. Binder, I want you to listen carefully. Mr. Martin asked the question. He asked for your recommendation about whether there should be any amendments to the act. He didn't ask about what kind of evidence we were about to hear, or from whom we were going to hear it. You seem to think it quite natural that the Privacy Commissioner is going to give us her recommendations about how she thinks the act should be amended. I think it's fair to say we think it quite natural that the department should give us recommendations about the things they agree should be recommended. It isn't just me; you've just heard it from Mr. Martin.

Mr. Martin, that takes no time from you. Go ahead.

Mr. Pat Martin: Thank you. That actually helps.

Further to that, if you could respond to the chair's input, I was wondering what it would look like if we embraced this as something we should do to PIPEDA. The question put here by our researcher is, would non-notification be a breach that you could file a complaint to the Privacy Commissioner about—for instance, if my Visa had been compromised, even if the company fixed it and it didn't cost me a penny, but they didn't inform me. Do you think that is something I should be able to complain to the Privacy Commissioner about, either as a class action or as an individual?

Mr. Richard Simpson: I can jump in.

You probably can complain right now to the Privacy Commissioner if you have reason to believe your personal information was somehow accessed by someone without your knowledge or consent, even if it was purely accidental or an act of someone with deliberate intention to subvert an information system. The reason you can do it is due to the ten principles of the CSA code, which the Privacy Commissioner is responsible for enforcing and companies and organizations are responsible for administering. It requires organizations to take proper security, proper steps to secure the personal information that is in their hands. Negligence, or an inability to protect that information, is really no justification or excuse for not complying with the act.

The issue you're raising is one that I think the committee is going to hear about from other people. It has risen in the United States, as your researcher has pointed out. There are a number of states in the U.S. that have adopted duties to notify, or breach notifications. There are various terms for it, I think quite a few—over 30. They have different approaches. One of the difficulties is that it is state by state, and therefore quite fragmented, across the U.S.

That's an issue that has come up in our consultations and that I think will come up before the committee. But it's not black and white that there is nothing there versus a duty to notify. In fact, there are a number of obligations under PIPEDA that organizations should comply with. In your case, to take that example, you would be able to go to the Privacy Commissioner. The difference is, as Michael Binder pointed out, that there is no obligation to notify everybody in a public way, which is what most of the laws in the U.S. do require.

•(1630)

The Chair: You have one minute.

Mr. Pat Martin: Very quickly, another serious concern raised by our researchers has to do with the effect of the Public Safety Act when it was passed into law and the necessary amendments to PIPEDA. It's a real concern that you could have the state getting the private sector to collect personal information for the sole purpose of telling government what that information is—in other words, contracting that out.

In what context does this come up? I guess one of the contexts—to preface that, even though there's not much time—is that in the province of Manitoba they contracted out health information to Manitoba Data Services Inc.. They did it so well that it became interesting to an American company, so an American firm bought it because it had a guaranteed anchor tenant. So now my personal health records are held in Dallas, Texas, by some company.... I have no idea how many times it's been flipped from owner to owner to owner, and I don't know what they're doing with that information.

Maybe I can change the angle of my question. Is there any way for the duty to follow the money, as it were, out of the country in the same way as we do with child sex laws or mining laws—Canadian activity operating outside the borders? Can anybody help me with my personal private information that's being held in Dallas by a private company?

Mr. Richard Simpson: The way PIPEDA works now under an accountability arrangement, as they call it, is that the Privacy Commissioner will investigate that situation from the point of view of the Canadian organization that first allowed your information to leave the country. So what—

Mr. Pat Martin: So there's still some obligation on the part of the government who sold it to the private firm? No. The private firm that sold it to the Americans would still have an obligation to me?

Mr. Richard Simpson: The organization that provided your personal information—

Mr. Pat Martin: Manitoba Data Services, I think it is.

Mr. Richard Simpson: Well, if you're talking about Manitoba Data Services, that's a little more difficult as an example because that's governed by a provincial privacy act. If we can take a private sector organization, though, that would have personal information that it collected from you, with your consent, for a particular purpose, the obligation on that organization, no matter how it decides to process that information and use it in the conduct of its business, which you have consented that it could do, is to protect that information in contractual form with any other organization that has access to it.

Mr. Pat Martin: So it does follow—

The Chair: Mr. Martin, your time is up. I can't allow you to interrupt again.

Just finish off your answer, Mr. Simpson, and we'll go to the next questioner.

Mr. Richard Simpson: It's an obligation that is transferred from the Canadian organization that is following PIPEDA and the principles under PIPEDA to make sure that a third party, no matter where that third party is located, must, by contract and therefore by law, respect the same principles as are in PIPEDA. So it's by extension.

The Privacy Commissioner will outline the same approach for you when she appears, I think, but she may have issues to discuss with you in terms of whether that covers all situations and how effectively it covers it in relation to a situation of public safety, for example.

•(1635)

The Chair: Thank you.

The last questioner from the first round is Mr. Tilson. Then we'll go to Mr. Peterson, followed by Mr. Stanton on round two.

Mr. Tilson.

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

I'm going to pursue the same line of questioning as the chairman and Mr. Martin.

We're actually looking to you for advice. You say you're looking to us for advice; we're looking to you for advice. You've indicated you've had meetings with stakeholders, and I assume you've had some discussions with the Privacy Commissioner.

I'd be interested in getting a list of the proposed or recommended amendments or suggested amendments that you would recommend the committee in turn recommend to Parliament as to where we should go with this, as opposed to our giving it to you. I think it's the other way around. We're charged with reviewing this matter and making recommendations to Parliament and we need your advice.

So I'm going to ask you—I can't believe you haven't sat down and said yes, we should have the following proposed amendments—will you give us that list?

Mr. Michael Binder: I hate to repeat myself, but you have to ask the minister to do this, because it's only the minister who can actually propose amendments and changes after the internal due process.

I'm not authorized to give you what I personally think is the amendment here.

Mr. David Tilson: All right.

Under Bill C-2, the proposed accountability legislation, VIA Rail, CBC, and a third one—which I can't remember—were moved to the Privacy Act, and it's not covered by PIPEDA. The Privacy Commissioner has indicated that she is concerned about this, and there will be lesser protection under the Privacy Act as opposed to PIPEDA.

Could you please comment?

Mrs. Danièle Chatelois (Privacy Policy Analyst, E-Commerce Policy Directorate, Electronic Commerce Branch, Department of Industry): From what we understand, this proposal was removed from the last version of Bill C-2, and now only the Enterprise Cape Breton Corporation is scheduled to be moved over to the Privacy Act.

This was originally done by an order in council on August 31, in which the Enterprise Cape Breton Corporation was removed from PIPEDA. It had originally been brought under the act by an order in council at the end of 2000. It was removed by an order in council in August 2005 and brought under a schedule to the Privacy Act at the same time.

Now, as we understand it, Bill C-2 is only proposing to formalize this in law for the Enterprise Cape Breton Corporation. We understand—

Mr. David Tilson: What I've just told you isn't correct. Is that what you're telling me?

Mrs. Danièle Chatelois: I don't want to appear—

Mr. David Tilson: I don't mind. I'm wrong a lot of times, so don't mind telling me I'm wrong.

Mrs. Danièle Chatelois: I want to tell you about a verification at council that I did with different versions of that bill. From what we understand, the version that went to first reading had those organizations in there. Upon reading the version that went to the Senate, we didn't see them anymore.

Mr. David Tilson: Okay.

I have a question with respect to the estimates. We went through the commissioner's estimates last week, or recently, and we heard that they're spending \$1 million on consultants in six months. Does the Office of the Privacy Commissioner have sufficient resources to handle what it's supposed to do?

• (1640)

The Chair: Insofar as this—

Mr. David Tilson: No, Mr. Chairman, leave me alone on this.

Some hon. members: Oh, oh!

Mr. David Tilson: If I'm going to get into trouble, I don't need you to help me.

Mr. Michael Binder: As a good bureaucrat will tell you, there's never enough money.

Mr. David Tilson: I assumed you would give me that answer, but we're spending a lot of money on consultants, so I assume from that... I don't know what I should assume from that.

Mr. Michael Binder: You will have to ask her. We're not in a position to—

Mr. David Tilson: Yes, okay.

The Office of the Privacy Commissioner is making a number of investigations and audits. Should the Office of the Privacy Commissioner be quasi-judicial?

Mr. Michael Binder: Maybe I don't understand the terminology. I thought it was quasi-judicial now. They have some legal powers or authorities—maybe in certain minds not enough.

Mr. David Tilson: Do they have adequate authority?

Mr. Michael Binder: You're going to hear some people say yes and some people say no.

Mr. David Tilson: What do you think?

Some hon. members: Oh, oh!

Mr. Michael Binder: I would have to ask my minister about this.

Mr. David Tilson: Okay.

Can you tell me what the relationship between your office and the Office of the Privacy Commissioner is? Is it a good relationship?

Mr. Michael Binder: We are the policy people, if you like, in overseeing the order in council, the provisions, and the act's ability to create regulations—for example, to deem substantially similar pieces of legislation in the provinces, to deem investigative bodies. We deal with a lot of regulatory issues.

The actual administration of the act is run by the Office of the Privacy Commissioner.

Mr. Richard Simpson: We work very closely with the Office of the Privacy Commissioner in a number of areas, including the Governor in Council's responsibilities that were just mentioned.

If you look at the policies for considering laws as substantially similar, the Office of the Privacy Commissioner has a specific role in terms of her point of view on those issues, as well as on investigative bodies. So there is a relationship, both informal and formal, to the extent that these are incorporated in policy guidelines.

We also work very closely with her on international issues. As I mentioned before, the OECD is very active in this area, and it continues to be very active. It's one of those bodies—to get back to the question raised by Madame Lavallée—where it's not so much that new norms are being established for privacy protection, but that areas of cooperation for cross-border enforcement of privacy laws and some of these international issues are being addressed. The Privacy Commissioner has actually been active with the OECD, working with us to look at some of these issues on an international basis.

The Chair: Okay.

Mr. David Tilson: All seven minutes have gone by?

The Chair: Eight minutes, actually.

This is a heads-up, ladies and gentlemen. We will be calling the minister, and we would ask you to get working on what he's going to say here. We will be asking what specific amendments, if any, he wants us to consider. And if he says none, we'll be asking his opinion of amendments that have been suggested by others.

We're now going to Mr. Peterson.

Hon. Jim Peterson (Willowdale, Lib.): Thank you.

Have you heard from any parties that the Privacy Commissioner should not have order-making power?

Mr. Richard Simpson: Yes, we have. As we mentioned earlier, there are really two points of view on the question of order-making powers or the Privacy Commissioner as a quasi-judicial body.

By the way, I'm sure you'll hear from the Privacy Commissioner herself on this issue. I think that should be the first point of contact about whether the powers are—

Hon. Jim Peterson: So there are two sides to this issue.

Mr. Richard Simpson: Yes, there are.

Hon. Jim Peterson: Okay.

Now, if PIPEDA is working so well, I can't figure out why we have four provinces that passed similar legislation after ours. Is this not overlap and duplication of the worst order?

• (1645)

Mr. Richard Simpson: Actually, the provincial legislation creates a comprehensive standard for protecting privacy across private and public sectors in those provinces. It really strengthens privacy protection in a way that either the federal law on its own or individual provincial laws could not do. Therefore, that was something—

Hon. Jim Peterson: If PIPEDA is protecting private sector information, why did the provinces have to step in and do it as well?

Mr. Richard Simpson: PIPEDA would not protect all elements of personal information. There are elements that are outside of the federal government's constitutional authority under trade and commerce—

Hon. Jim Peterson: Such as a provincially owned agency or a provincial government or department.

Mr. Richard Simpson: Yes, such as the health sector. There are a number of areas. Any area where information is not defined as commercial cannot be captured by PIPEDA. Therefore, there are areas that—

Hon. Jim Peterson: Why do provincial laws cover commercial information, then?

Mr. Michael Binder: There is no duplication; it's either one or the other. The moment they pass their law, we are out of it.

Hon. Jim Peterson: I know that.

Mr. Michael Binder: Some of them wanted a more comprehensive approach to what's happening in their own jurisdiction. Some provinces have decided to go with PIPEDA, and so far they have no intention of passing a provincially based law.

Hon. Jim Peterson: There would be holes in their structure, then, for government operations, I suppose.

Mr. Michael Binder: There could be, and I guess they'll cross that bridge when they come to it. Right now, they're quite happy to not enact it.

Hon. Jim Peterson: What's happening in the U.S.? Does every state have a law similar to this, but there's no federal law? Is that the situation?

Mr. Michael Binder: There's no law like PIPEDA that's economy-wide, independent of various sectors. There you have health privacy, financial privacy, and those kinds of bills. I think there's also—

Mr. Richard Simpson: They're national?

Mr. Michael Binder: They're national, yes. But then I think there's some provision in various states. So you're really talking about complexity. It's very complicated there.

Hon. Jim Peterson: It's also complex for foreigners doing business in Canada, with provincial and federal laws to comply with.

Mr. Chairman, I'd just like to get a sense of how many witnesses.... Have a lot of people applied? How many?

The Chair: Mr. Clerk.

The Clerk of the Committee (Mr. Richard Rumas): Approximately twenty, and that includes individuals and groups.

Hon. Jim Peterson: That's a fairly high number for this committee.

The Chair: It surprised me—on this act. I'd never even heard of it.

Hon. Jim Peterson: We would welcome your giving us the names of some witnesses we perhaps should call before us. That would be very helpful to our committee.

Mr. Richard Simpson: We have a list. We can make that available to the clerk.

The Chair: Is that it, Mr. Peterson?

Mr. Stanton.

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chairman, and thank you to our witnesses here this afternoon.

I have only five minutes, so I'll try to get through this as quickly as I can.

I have a question from some earlier comments that were exchanged on this notion of the work product. You mentioned the release of personal information as it relates to medical information for.... Just to clarify, you didn't mean of patients, I assume, but of people involved in the professional activities. Could you clarify what you meant by that? Prescription information, I think, is what you talked about.

You were not talking about prescription information or identifying the individual who is prescribed a certain pharmaceutical. That information is clearly in the personal realm, is it not?

Mr. Richard Simpson: That's correct. This was more the personal element to that. On one side of this argument was the doctor making the prescription, and his name was there. As I understand it, the key issue was whether that was personal information and should be protected or whether it was a work product, because this is in his capacity as a physician.

• (1650)

Mr. Bruce Stanton: I appreciate that clarification.

To go to another completely different area, from another committee that I'm working on in regards to the Internet, there is just dreadful use of the Internet in the realm of crime—in this case, the issue of sexual exploitation and human trafficking. The Internet is being used for these scurrilous purposes. I note that under section 7 there are exemptions and consent for issues relating to crime, fraud investigation, law enforcement, security, and so on.

Are there any aspects of PIPEDA that are not working with respect to giving the law enforcement community the access it needs to investigations, prosecutions? I assume there would typically have to be subpoenas or warrants provided before law enforcement could get access, for example, to the names and contact information of certain Internet subscribers. Are there any issues around that, or should there be some improvement of PIPEDA as it relates to allowing law enforcement to do its job?

Mr. Michael Binder: We have a specific carve-out for investigation purposes and crime fighting. Quite honestly, we have not had any complaints. Anytime there was a deficiency, it was amended. There was an anti-terrorism kind of provision that was passed.

Mr. Bruce Stanton: That would certainly be important to know, because all of those names and addresses, of course, are kept in the commercial, private companies...in this case, Internet security providers.

Finally, in the area relating to the powers of the Privacy Commissioner herself, as you went through the deck you mentioned there were penalties, remedies, fines that could come into place. I assume that's only through the Federal Court, so her only means to enforce the act is through the courts. I was trying to think of some other examples where there might be other forms or powers brought to the table. Presumably in other departments there are regulations, there are enforcement officers and that sort of thing, people who work in the field, who can apply regulations.

But I'm wondering where we could possibly see some greater ability on the part of the Privacy Commissioner to get results in the field, other than having to resort to the Federal Court. Are there some other examples where an office like this might have better means to do that?

Mr. Michael Binder: There are quasi-judicial bodies with different powers, like AMPs—administrative monetary penalties, I think they're called, which can actually impose penalties, severe penalties, directly. You would have to have a legislative change to do that.

Mr. Bruce Stanton: Is that the sort of tool that could in fact be incorporated under PIPEDA, then?

Mr. Michael Binder: Not right now. You would have to amend the act to actually provide it with that particular power. There are going to be some advocates who come in front of you and suggest strongly that this should be done.

Mr. Richard Simpson: So there would be a fundamental change to how the act operates, because it does operate now under the ombudsman model, with the Federal Court being the instrument the Privacy Commissioner uses to go after, as I said before, very deliberate and intentional violations of the act. So it's very much the order-making or oversight and redress issue that we talked about earlier.

The one issue that will come up under a scenario of order-making powers is whether you still need to set up some kind of independent body that would actually apply the penalties. For example, the Canadian Human Rights Commission has a tribunal. The Competition Bureau has a tribunal. So you ensure that the investigative body does not have the right to be both judge and jury.

The Chair: Thank you.

I have just one question to follow up on Mr. Stanton's. We recently had a case in southern Ontario, in St. Thomas specifically, where the father was alleged to be abusing his child online. The police were trying to prevent that crime from continuing, so they called the server to ask for the name and address of the person. I gather that there was some reluctance by the server to give up that information. Would the reluctance by the server have been under PIPEDA—by the way, Mr. Simpson, I prefer that pronunciation, so I'll go with you—or would the alleged concern of the provider have been under the Privacy Act? Which of those two would it have been?

• (1655)

Mr. Richard Simpson: In some cases there is an issue around what constitutes lawful authority. As we said earlier, the act is pretty clear that if you have lawful authority for that information as part of an investigation of criminal activity, national security, or whatever, those requirements are above the protection of personal information. In operational terms, there's sometimes a question about what is lawful authority. Is it a warrant? In some cases on the Internet, when you're moving very quickly, law enforcement cannot produce a paper warrant. Sometimes they're contacting you electronically.

So these are the kinds of issues I think you would hear about if you talked to both privacy advocates and to the law enforcement community in terms of an operational requirement. How do you define lawful authority in a way that ensures that the balance is struck?

The Chair: Thank you very much.

Monsieur Laforest, s'il vous plaît, cinq minutes.

[Translation]

Mr. Jean-Yves Laforest (Saint-Maurice—Champlain, BQ): Thank you, Mr. Chairman. I have two questions for the witnesses.

Mr. Simpson, you tabled a document in which you refer, among other things, to the Quebec constitutional reference. You note the following on page

15: As “substantially similar” to PIPEDA, the Quebec privacy law continues to apply within the province.

Are you saying that if the Quebec law were not substantially similar, it could not continue to apply within Quebec?

My second question pertains to the next paragraph in which you say this: Decision will confirm the federal government's ability to exercise its powers over trade and commerce [...]

Are we to assume from this that a decision will be forthcoming and if so, that a responsible official in Quebec would say that the decision handed down supercedes the federal government's authority in this area? I realize that a decision may not necessarily say this, but isn't there an assumption here that there will be some sort of decision, even though one has not already been handed down?

Mr. Michael Binder: We've just discussed that point. You are correct. The expression “will confirm” is significant. It will clarify the situation.

Mr. Jean-Yves Laforest: I would have preferred to see “will confirm the limits”.

Mr. Michael Binder: Or “will clarify”.

Mr. Jean-Yves Laforest: The document says that the Quebec law is “substantially similar” to PIPEDA. Does that mean that if the law was not substantially similar, it could not continue to apply?

Mr. Richard Simpson: That question has to do with the federal act. If a provincial law was not considered

[English]

substantially similar,

[Translation]

the federal act would continue to apply within the province and organizations would not be excluded from the federal act's application. If I can continue in the other language, I would say that

[English]

it's more a question of the federal law and whether it would exempt organizations, rather than whether the provincial law would continue to apply. It would continue to apply regardless.

• (1700)

[Translation]

Mr. Jean-Yves Laforest: Is this not confirmation of an infringement on constitutional jurisdiction?

Mr. Michael Binder: No. We're dealing with a hypothetical situation. This law was drafted using the Quebec model for inspiration. The policies and ideas are derived from the Quebec act. Quebec was the first province to adopt similar legislation. If

Quebec wanted to amend its legislation and remove, for instance, the provisions respecting consent, then we would object because personal information on Canadians must be protected by law. In this instance, they will be protected by two separate laws.

Mr. Jean-Yves Laforest: Ms. Lavallée has a short question.

Mrs. Carole Lavallée: Mention was made earlier of the report by Privacy International. I assume that you've read it and that you have a copy of it in your possession. Could you possibly forward it to us?

Mrs. Danièle Chatelois: Yes. A table and a summary are available and we can send them to you.

Mrs. Carole Lavallée: Thank you.

[English]

The Chair: Thank you very much.

Mr. Wallace.

Mr. Mike Wallace (Burlington, CPC): Thank you, Mr. Chairman.

Thank you for being here late in the afternoon.

I want to know what Bruce Stanton is hiding. I want to know what his prescription is.

Mr. Bruce Stanton: I'm not telling you.

Mr. Mike Wallace: I agree with the chairman and my colleague. Maybe it's because of my previous experience as a municipal councillor, but my expectation was that staff, which I consider you to be, would give us recommendations on areas that we know nothing about—unless you're involved with it, you don't know a lot about it—but obviously that's not the case.

My question is for future reference. Since this is a required review, not something that somebody here on the committee is interested in doing.... I wouldn't say it's that political, since you had consensus to make it happen. Would we have been better off to have the minister here first—since it sounds like you work for the minister—and pose the questions we need answers to from the ministry, or should we have had permission from the minister to allow you to provide us with recommendations?

I'm new here, so this is all new to me. I'm interested in your comments, if you can still talk about it, on what a better process for us would have been.

Mr. Michael Binder: We may have misunderstood the requirement, but we were told very specifically that we were called here to provide an overview of the bill. It's like PIPEDA 101.

If you had asked for a recommendation, we would have reacted by either seeking authority to give you a recommendation, or by telling you we could not do it and seeking your guidance on inviting the minister. But this was to be a purely academic overview of the meaning of the act, its provisions, etc.

We took notes. If you want, we can go back and see what we can tell you about our personal views, and then get back to you on this.

Mr. Mike Wallace: I appreciate that, because we haven't had the commissioner here yet on this particular topic. But in a July 2006 report, she says, "It is not the role of this Office to draft proposed amendments to PIPEDA." So if we're not getting it from her and we're not getting it from you, I'm not sure, other than stakeholders, who we'd get it from, in terms of some direction. It's just my past experience.

In the deck you've provided here, you have suggested a number of what you have defined as minor amendments. These are the areas that you think we will get minor amendments in. Is that an accurate statement?

Mr. Michael Binder: Yes, we believe that the support witnesses you have on your list will probably propose some of those amendments. So we'll give you a heads-up. That's our understanding of what's coming in front of you.

Mr. Mike Wallace: Okay. So we can focus our attention on those areas, and then that would be accurate.

I have a question for you, if I still have some time. Is it possible to get a review of the strengths of PIPEDA? I think there are four provinces that have their own privacy information system. I didn't see in here which one's stronger, what we like, and what we don't like in other ones. Are there things we should be adopting that the provinces adopted? Or should we be getting out of the way of the provinces? I'm not sure where we're headed with that.

For example, I had consultants in to see me about the definition in the British Columbia model. Is it a better definition or not? How do we find that out from you guys? Do you have opinions on those things?

• (1705)

Mr. Richard Simpson: We certainly can provide some indication of where provincial privacy acts—except for Quebec's, of course, which came after the federal law—have addressed some issues, like the work product issue, in interesting ways, which you might want to look at, based on what you hear from other witnesses. We're also suggesting, in response to your request for people who should be called before the committee, that provincial privacy commissioners are excellent people to discuss not just the application of their legislation, but also privacy protection in general and the way in which the regime for privacy protection works in Canada generally.

So I think in both ways we can provide some help ourselves in terms of some of those areas. But I think you'd best get it from the horse's mouth, so to speak. If provincial privacy commissioners are going to appear before the committee, then they'll give you an excellent review of how elements of their legislation are substantially similar to the federal law, and areas where they have a couple of ideas that you might want to consider.

Mr. Mike Wallace: I appreciate that.

Those are my questions, Mr. Chairman.

The Chair: Just for the committee's information, all of the privacy commissioners were invited to appear. Three declined, and the British Columbia commissioner will be here.

Mr. Martin, do you have any questions?

Mr. Pat Martin: No, thank you.

The Chair: Madam Jennings.

Hon. Marlene Jennings (Notre-Dame-de-Grâce—Lachine, Lib.): *Merci beaucoup, monsieur le président.* Thank you very much.

I'm not a regular member of this committee but I've been watching out for the review of PIPEDA since it first came into legislation, because when it was first tabled by the previous government, it was brought before the industry committee and I was a regular member of the industry committee. I'm quite proud of the fact that some of the amendments that were brought at that point and actually became legislation came from the Liberal side, and some of them, in particular, from me—the whistle-blowing protections, for instance, strengthening the actual protections and powers and authority of the commissioner.

There were two issues that were major at the time the industry committee reviewed this legislation at second reading and actually brought amendments. One was the actual privacy protection for personal information or information generated through the exercise of individual professional responsibilities, what we now call work product information. There was a real concern on the part of many of the stakeholders that the definition that we had in PIPEDA was not sufficient and that in fact it would end up being an impediment.

Following the coming into force of this legislation, because the government basically convinced the members of the committee at that time, no, no, it's fine, work product won't be a problem; the definition, even if it's not there...everybody understands that there isn't that privacy protection for work product information and therefore the current definition will not be an impediment. In fact, that's not the case. There have been cases that have gone to the courts. And the previous commissioner has actually had to issue an interpreted ruling, which has been and can be challenged before the courts.

So I think that the issue of looking at that specific definition and making a distinction between personal information and work product information and removing the privacy protection for work product information is very important. I'm really heartened by the fact that members of this committee are asking these questions, and I assume from this deck that the consultations you have had with stakeholders has raised that. And if your minister gives you permission, you will be able to come forward with recommendations or, through the minister, recommendations on that specific thing. Am I correct?

Mr. Richard Simpson: Always! You are correct.

Hon. Marlene Jennings: Well, put it this way: I'm going to attend as many of these meetings as I can, even if I have to strong-arm some of my Liberal members not to come so I can legally replace them. And I'm going to try to convince them that if the government doesn't come forth with an amendment, they should come forth with a specific amendment to make that distinction.

The second issue I had concern with at that time was the issue of consent, providing consent, express consent, implied consent, to companies that actually collect information and then may share it with their divisions or with third parties that they have contracts with, or whatever. I'm aware of a study that was recently done by the institute over at the University of Ottawa on the whole issue of consent, and my hair went straight when I saw the results.

There's a real problem on the definition of consent, what's express consent, what's implied consent, what kind of consent is required in order to share that information with third parties, what kind of information is actually being shared. There's a real problem there. And not all companies, apparently, have put into place an actual protocol. For those that have, that protocol may not be easily accessible by the consumer who's being asked to sign away their personal information. So I'm assuming that's another issue that you have consulted on with stakeholders, and that you have a clear vision of recommendations you'll be bringing to the minister. I'm assuming you'll be recommending to the minister that he either come prepared to answer that or that he release you from your confidentiality and allow you to answer directly to this committee.

Am I right about that?

• (1710)

Mr. Richard Simpson: We know about the study that you mentioned, and yes, if I had enough hair, mine would stand up on end also. It is discouraging to hear the results of the poll like that, or the study.

What it points to, though, is not only the definition of consent, because that's certainly part of it, but it's also a question of how aware organizations are of their responsibilities under the legislation, whether it's provincial or federal, and that's something we need to address. I'm sure the Privacy Commissioner, because she has done it, she has addressed it in her annual report to Parliament, would want to talk to you about the educational component.

Hon. Marlene Jennings: Thank you.

Chair, do I have any more time? I've been trying to talk fast—

The Chair: No, I'm afraid you're out of time, but it was well worth the five minutes. We do welcome your participation, Ms. Jennings, particularly since you were on the original committee. It's very helpful.

I don't have a formal list. Would someone from the Conservative side like to put up a hand? No?

Then we'll go to Madame Lavallée.

[Translation]

Mrs. Carole Lavallée: Mention was made of the Quebec law and of the federal act. I'd like to know the current situation in Quebec. As a rule, Quebec law applies in Quebec, but in the case of businesses and organizations under federal jurisdiction, in particular banks, does the federal act apply?

Mr. Richard Simpson: Yes, it does.

Mrs. Carole Lavallée: That's how it works?

Mr. Richard Simpson: Yes, the federal act applies to banks, broadcasters, and so forth.

Mrs. Carole Lavallée: To telecommunications, ports, airports and so on. We're talking about the usual list of operations.

Ms. Alexia Taschereau: That's right.

Mrs. Carole Lavallée: They are covered under the federal act.

Ms. Alexia Taschereau: Yes.

Mrs. Carole Lavallée: Thank you. I have nothing further.

[English]

The Chair: Mr. Peterson.

Hon. Jim Peterson: I would like to turn the rest of my 20 minutes over to Ms. Jennings, please.

Voices: Oh, oh!

The Chair: Ms. Jennings.

Hon. Marlene Jennings: I love my job.

With regard to the points raised by Madame Lavallée and Monsieur Laforest, this was a major piece of contention before the industry committee at second reading. It was quite interesting, because all of the constitutional experts came in and explained very clearly that under the Canadian Constitution you have areas that are exclusively federal jurisdiction, you have other areas that are exclusively provincial jurisdiction, and then you have areas that overlap, where both authorities, both levels of government, have constitutional authority to legislate. Where they bump up against each other, or if they do, the federal government may have to withdraw.

In this particular case, they made it clear that if no provincial law was regulating the protection of personal information in e-documents for the companies and organizations regulated provincially within the territory of a province, then the federal government's PIPEDA could apply there. However, even where there was provincial legislation, as soon as the information took part in a commercial transaction that crossed provincial borders or went outside our country borders, then it was the federal government that had clear and exclusive jurisdiction.

I'm amazed that five years later this same bogus argument is being brought up by my esteemed colleagues—who I respect very much, but I had the same argument with Madame Lalonde on the industry committee. The constitutional experts, including those from Quebec, said very clearly that if I buy something at a company in Quebec and I'm a resident of Quebec, and that company sends my information because its supplier is in B.C. or in the United States, Quebec law doesn't protect me. As soon as my information crosses the border, it would be in la-la land, and they could do anything they wanted. That was why there was a necessity for federal legislation.

As was stated, this legislation was modelled in large part on the model that already existed in Quebec. It was kind of like what we tried to do with

•(1715)

[*Translation*]

the national day care program. A program was already in place in Quebec. It took some time to convince provincial governments to sign on, but ultimately agreements were concluded. These were patterned on the Quebec model. PIPEDA took its inspiration from the Quebec model, but is designed to protect the sectors and areas not covered under the Quebec law.

[*English*]

Let me take my breath here.

The Chair: Yes, that was a three-minute speech. Do you have a question, Marlene?

Hon. Marlene Jennings: Amazingly, I do.

The Chair: Because you could do it another time, too.

Hon. Marlene Jennings: *Non, merci.*

On the question of mergers and acquisitions, I see there have been requests for amendments to the consent requirements. Could you give us a little bit of information on what are these requests?

You're not giving a recommendation, so I'm assuming you don't have to go to your minister. It's simply sharing with us requests that you're aware of for amendments to PIPEDA on the consent requirements dealing with mergers and acquisitions.

Mr. Michael Binder: The way I understand it, when you do a merger or an acquisition, you need to have some data and information about officers, about the business they're in, and so

on, and some of this information needs to be—the argument goes —“access without consent”, because otherwise they'd become aware of what's going on. So there are those kinds of issues here. Again, you're going to hear the other side of the argument, that it's because of this personal information that you don't want to share those arguments.

Hon. Marlene Jennings: Okay, thank you.

I'm done for today.

The Chair: I think we all are.

Colleagues, I'd like to go in camera briefly, in a minute, after I thank the witnesses.

You were right, Mr. Binder, we did ask you for a PIPEDA 101. That's absolutely correct. But as part of that consideration, because we're mandated to review the entire act, I guess we just assumed that the department, as a result of its consultations, might have some recommendations for us. So we're not looking to criticize you; we're now giving you some guidance as to what we're looking for, and specifically now what we're looking for from your minister. But you're absolutely correct that we did want a 101 course, because only one of us was on that committee when it was first passed. So we did want to get some background and contextual ideas on it.

Thank you so much for coming and for answering our questions. No doubt we'll see you again with your minister.

I'll suspend the meeting for two minutes.

[*Proceedings continue in camera*]

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>**

The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.

Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.