House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 019 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Monday, November 27, 2006

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Monday, November 27, 2006

● (1530)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): Good afternoon, colleagues.

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 conducting a statutory review of part 1 of that act.

Today our witnesses, from the Office of the Privacy Commissioner of Canada, are Ms. Jennifer Stoddart, Privacy Commissioner of Canada; Heather Black, assistant commissioner, PIPEDA; and Melanie Millar-Chapman, strategic research and policy analyst.

Welcome to you.

We understand, Commissioner, that you have an opening statement and then we'll go into the usual questioning. Is that correct?

Ms. Jennifer Stoddart (Privacy Commissioner, Office of the Privacy Commissioner of Canada): If it's convenient for you, Mr. Chairman, I have a fairly short opening statement and then we'll have a good time for questions.

[*Translation*]

Ladies and gentlemen members, I am very pleased to be here today to assist you with your review of the Personal Information Protection and Electronic Documents Act, or PIPEDA, as it is commonly called.

Our privacy is fundamentally important to all of us—as consumers, as citizens, as students, as employees—in every aspect of our day-to-day lives. PIPEDA, along with the Privacy Act that applies to federal departments and agencies, provides the foundation for privacy protection in Canada.

I would like to take a moment to explain why PIPEDA is more important than ever. When we first started talking about this law in 1998, the Information Highway was a catchphrase; now it is a reality. Transborder flows of personal information were a trickle. Now they are a flood. New and emerging technologies such as location tracking devices and radio frequency identification threaten privacy in ways that were unimaginable a decade ago.

We want to help you in this critically important task of ensuring that PIPEDA remains capable of dealing with the many privacy challenges we face in the 21st century.

In preparation for the review we issued a consultation paper setting out twelve issues that we identified as worthy of attention. We received over 60 submissions from a variety of organizations and individuals. A summary of the submissions along with a discussion of the issues we identified are included in the submission we have tabled with the Committee. I think it is fair to say that there is general agreement about the issues the Committee might want to consider, but unfortunately there is no consensus about the best way to address all of these issues.

[*English*]

I have a very clear and positive message that I want to leave with you today. We believe that PIPEDA is generally working well. PIPEDA strikes a careful balance between two goals: the right of individuals to keep their personal information private, and the need of organizations to collect, use, and disclose personal information for purposes that a reasonable person would consider appropriate.

I've chosen the following issues to bring to your attention today because they have the potential to affect the privacy interests of a large number of Canadians.

First of all, it is important that privacy law be administered in a stable context. PIPEDA is based on an ombudsman model. As Privacy Commissioner, I have the power to investigate complaints, to conduct audits, to make findings, to issue non-binding recommendations, and to initiate court actions. We will not be asking for enhanced enforcement powers. We are not convinced that the time is right to make such a fundamental change to the enforcement mechanisms for several reasons, both practical and administrative.

Secondly, some of the most difficult complaints we have received have involved employee information. PIPEDA is based on consent, which is a challenging concept in a workplace environment where there is unequal bargaining power. One of the issues that you may wish to consider is whether there are more appropriate ways to deal with employee information without sacrificing the privacy rights of workers. Our submission offers some suggestions about dealing with employee information.

With respect to the issue of work product, PIPEDA does not use the term. We've addressed this issue by adopting a case-by-case approach to assessing whether or not the information in question is about the individual. If the answer is yes, then the information is protected by the act. We recognize that an individual in his or her capacity as an employee or as a professional may generate information that is not about the individual. We would caution you that removing all such information from the act could result in intrusive workplace monitoring and other abuses.

● (1535)

[*Translation*]

Since the Act was passed, concerns about protecting transborder flows of personal information have taken on a new urgency. As a result of globalization, the emergence of new "follow the sun" business models and the explosion of offshore processing, the amount of personal information flowing across borders has increased dramatically. At the same time, governments are increasingly interested in obtaining access to this information for national security purposes. PIPEDA does not contain any specific provisions with respect to transborder information flows. We believe that by providing guidance, requiring organizations to be open about their processing practices and holding them responsible for personal information when it crosses borders we can address the challenges of transborder information flows.

We also need to ensure that we can deal with complaints that involve other jurisdictions. We live in a world of increasingly virtual borders in which privacy issues do not always respect national boundaries. I would ask you, ladies and gentlemen, to consider a specific provision to make it clearer we have the authority to share information with our international counterparts while cooperating on investigations of mutual interest.

The act requires organizations to protect personal information from unauthorized access or disclosures. The Act does not require organizations to take any specific actions in the event of an unauthorized disclosure. More than half of the U.S. states have passed laws requiring organizations to notify their customers or clients when their personal information has been compromised. Policy makers in the European Union are looking at similar requirements. Breach notification laws may force organizations to take security more seriously. They may provide individuals with an early warning system to make them better prepared to deal with the risk of identity theft and other harms that might result from a privacy breach. We look forward to discussing with the Committee whether it is possible to fit a notification requirement into the PIPEDA framework.

● (1540)

[*English*]

Before concluding, Mr. Chairman, I'd like to raise one very specific and I think pressing matter that relates to a recent Federal Court of Appeal decision. This case deals with solicitor-client privilege and our ability to obtain access to documents in the course of our investigations. This recent decision in the Blood Tribe case leaves a gaping hole in our ability to conduct meaningful investigations. It effectively allows organizations to shield information from our investigators with no independent verification that the documents in question do in fact contain information subject to solicitor-client privilege. Although we are seeking leave to appeal, we believe this ambiguity in the legislation needs to be clarified with an amendment to PIPEDA as soon as possible.

To repeat, we believe that PIPEDA is working reasonably well. Overall, we think that there is a high level of compliance and that the business community is committed to the protection of our personal information. Can the act be improved? Yes. Based on our experience in applying the law since 2001, and with benefit of the second generation private sector laws that have been passed in some provinces, we have identified in our submission gaps in the act and provisions that would benefit from greater clarity. We think there are ways in which the act can be made more practical and more predictable, so after you've had the benefit of hearing from, doubtless, numerous other witnesses you may call to appear before you, we would ask to come back at the end of your hearings, Mr. Chairman, in order to give our final view on the various matters being put before you.

Thank you.

The Chair: Thank you very much, Commissioner.

Now we will commence our first round of questioning. We have a full docket of questioners, who have seven minutes for this round. We'll start with Mr. Peterson.

Hon. Jim Peterson (Willowdale, Lib.): Thank you, Mr. Chair, and thank you, witnesses.

What types of amendments would you envisage to get around the Blood Tribe decision?

Ms. Jennifer Stoddart: They would be very specifically worded amendments that make it clear—and I think the model is in the Privacy Act—that our investigative powers are not blocked by solicitor–client privilege. This is in the Privacy Act. It was not put in PIPEDA, we understand, because it was thought that our investigative powers were clear enough. There seems to be some ambiguity, so we would look to the Privacy Act as a model.

Hon. Jim Peterson: Do you envisage any objections to that type of amendment?

Ms. Jennifer Stoddart: There might be, yes.

Hon. Jim Peterson: You've floated this suggestion before. Have you received any objections?

Ms. Jennifer Stoddart: No, we have not floated it before, Mr. Chairman. We only received this decision about three weeks ago, I believe. This is a decision of the Court of Appeal. The first level of the Federal Court was in agreement with us that our investigative powers included looking at documents for which it was alleged there was solicitor–client privilege. The Federal Court of Appeal disagreed with that, so this is now the first time we have asked for an amendment.

Hon. Jim Peterson: Can you give us some examples of how that's going to hamper you specifically in the work that you're doing?

Ms. Jennifer Stoddart: We think there is a very real possibility that respondent organizations could take a very expansive view of what solicitor–client privilege is, and thus in fact shelter documents containing personal information that would be appropriate to our investigation behind the use of this privilege.

Hon. Jim Peterson: Can you give us a sense of how many complaints your office has received since PIPEDA?

Ms. Jennifer Stoddart: Since the beginning of PIPEDA, I believe there have been about 1,400 complaints overall, Mr. Chairman.

Hon. Jim Peterson: Over three and a half years?

Ms. Jennifer Stoddart: No, over the five years that it has now been in force. Let me just find those statistics for you.

We have received over 56,000 written and telephone inquiries.

Hon. Jim Peterson: You can give us this information later.

Ms. Jennifer Stoddart: It's about 1,400.

Hon. Jim Peterson: Is there one type of complaint that dominates?

Ms. Jennifer Stoddart: The complaints are mainly about use and disclosure, collection, and access. Those three types dominate from year to year. First of all, use and disclosure ones make up 38%; collections are at 23%; and ones on access to one's own file, one's own personal information, make up 18%.

● (1545)

Hon. Jim Peterson: How many times have you had to go to court?

Ms. Jennifer Stoddart: I believe we've been involved in some fifty cases since the inception of the first stage of PIPEDA. We're currently at the Federal Court in twelve active cases.

Hon. Jim Peterson: How long do each of these cases usually take before there is final determination?

Ms. Jennifer Stoddart: That's hard for me to answer. I haven't really measured it.

Hon. Jim Peterson: I imagine it would be substantial.

Ms. Jennifer Stoddart: Before the Federal Court, you mean?

Hon. Jim Peterson: Yes. It would a substantial amount of time before you could get to court, be heard and be ruled on, wouldn't it?

Ms. Jennifer Stoddart: The statistics over the last five years show that, on the average, we have disposed of the complaints under PIPEDA in under a year. It's around eleven months, on an average. As you know, the time to go to Federal Court or the time before the Federal Court, of course, would then depend on how quickly both parties move, where the hearing is, and various other things like that.

Hon. Jim Peterson: In your excellent memo to us, you say you don't want order-making power because you want to continue on the course you're on. This means, then, that you're probably happy with having to use courts to resolve certain issues.

Ms. Jennifer Stoddart: Mr. Chairman, this is not the time to make any major changes in the framework of PIPEDA. As certain members of this committee will remember, this law was applied in less than ideal circumstances at the beginning. It has been a very difficult road for the Office of the Privacy Commissioner. That is one hand.

On the other hand, I don't think we have any really serious study about the advantages and disadvantages of various models of enforcement.

Thirdly, Mr. Chairman, I could say that we have quite a wide range of powers and that going to the Federal Court is in fact a very strong power, because an order of the Federal Court is an important order in the hierarchy of legal orders.

For all these reasons, I'm happy to go to Federal Court at the present time.

Hon. Jim Peterson: Even though it's slow and cumbersome and costly?

Ms. Jennifer Stoddart: Again, I say, I don't know. I have nothing that leads me to believe that this is slower or more cumbersome than going before equivalent tribunals, and I have some knowledge of tribunals from having administered tribunals. It depends on the requests for stay of proceedings, it depends on the availability of parties, it depends on where they can be heard. So I think there aren't excessive delays at the Federal Court. I don't think we have to wait excessively long to be heard. Most of our cases are settled out of court.

In fact, if I can conclude on that, Mr. Chairman, when we, as we have in the last year or so, have in essence turned up the heat and said if you don't comply to our recommendations and come into conformity with the law we will take you to Federal Court, I think all organizations but one have complied.

Hon. Jim Peterson: Two of the provinces do have order-making power, don't they?

Ms. Jennifer Stoddart: Yes.

The Chair: Thank you, Mr. Peterson. You were right on seven minutes.

Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Thank you very much.

First of all, welcome. Thank you very much for coming to present us your suggestions on updating the act. You make a number of suggestions which are immensely interesting and you indeed point out the current issues.

One sentence of yours sticks in my mind:

> [...] and the explosion of offshore processing, the amount of personal information flowing across borders has increased dramatically.

You also said — although I don't remember the exact wording — that there's currently no provision in the act for handling this confidential information. I'm not exactly citing your sentence; I don't know what paragraph it's in.

● (1550)

Ms. Jennifer Stoddart: As a result of the virtually global movement of personal information, that volume wasn't anticipated when the act was drafted in 1998. I don't have a clear directive in the act for dealing with my counterparts to solve potential problems. I'd like a change so that the act would give me a general scale to determine whether it's in the public interest to go and talk about even the details of a complaint brought before me with a counterpart in the European Union, for example, whether it's in the interest of Canadians' privacy.

Mrs. Carole Lavallée: Okay.

Currently, I imagine you have activities, meetings, conversations with people in the European Union or the United States. Don't you?

Ms. Jennifer Stoddart: Yes.

Mrs. Carole Lavallée: You already do. Then you have the... However, am I to understand that you want to go further in dealing and negotiating with them?

Ms. Jennifer Stoddart: We're trying as much as possible to address only very general areas, so as not to give out a person's personal information, for example.

However, we'd like some clarification. For example, in a complaint concerning an individual, where it's preferable that that complaint be addressed by our French counterparts, we'd like them to be able, in an entirely legal way, to have the individual's personal information as well. I'd like to clarify that.

Mrs. Carole Lavallée: I only want to be certain I understand. Pardon me, but I'm new to this committee. I haven't been examining this act for very long. So I want to make sure I clearly understand what you're saying.

In the case of a complaint, for example, you'd like to be able to deal with your counterparts in the European Union so that you could investigate the complaint together. Is that correct?

Ms. Jennifer Stoddart: Yes, that's it.

For example, we want to be able to simply send our counterparts a copy of the complaint including all the personal information of the person in question, telling them that they can find a remedy for our complainant here in Canada.

The act isn't clear on this point; it doesn't specify whether I can do that. I haven't done it to date. I stick to general information.

How could we reinforce the actions on both sides?

Mrs. Carole Lavallée: Okay.

I find that interesting, but I must admit that's not what I understood. That's not how I had interpreted your problems or concerns. I thought they focused more on the general way of protecting personal information of Quebeckers and Canadians where that information, for one reason or another, must circulate internationally. I thought that that was more your concern.

Ms. Jennifer Stoddart: Okay. That's another of our concerns. We say that in a brief. That's a question that has been the subject of a number of discussions. You'll no doubt hear a number of views on that question.

In our opinion, it's possible to include in the act general scales like those the Canadian government has included in the directives recently issued by the Treasury Board for the public sector. However, one of the principles of the act, the accountability principle, is also designed to encourage the businesses that export the personal information of Canadians to submit the other outside businesses or organizations to Canadian standards.

We're telling you that this is a major problem. We mention various approaches, and we add that, if you don't intervene, there is, in any case, a fairly strong and flexible principle, the accountability principle.

Mrs. Carole Lavallée: All right. To address this problem, you'd simply need additional measures in the act. Is that what you're telling me?

Ms. Jennifer Stoddart: We can already address this problem under the accountability principle.

Mrs. Carole Lavallée: Okay. When you refer to the accountability principle, are you talking about Bill C-2?

Ms. Jennifer Stoddart: No, I think it's principle no. 4.

Mrs. Carole Lavallée: Okay. You're really talking about a principle.

Ms. Jennifer Stoddart: Yes. These are the principles of the code. This act was designed on the basis of a standard of the code of Canadian standards. The Privacy Code is related to and forms an integral part of the act. The first principle of the act is the accountability principle.

Even if I'm a Canadian organization that sends personal information on Canadians outside the country, I'm still responsible for it here in Canada.

● (1555)

Mrs. Carole Lavallée: Okay. Perfect. I understand better.

You also refer to the disclosure of personal information, and you say it would be a good idea to include a requirement concerning notification in the act.

Ms. Jennifer Stoddart: Yes.

Mrs. Carole Lavallée: That isn't provided for in the act either.

Ms. Jennifer Stoddart: No, that's not provided for in the act. Perhaps at the time there hadn't been enough leaks from large data bases for anyone to think it was a problem.

Yes, we're in favour of the principle. The problem is in knowing how to implement it.

Mrs. Carole Lavallée: Okay. In the meantime, you must have formed an idea about how to implement it.

Ms. Jennifer Stoddart: We considered a number of American examples. That's one thing we should look at with government lawyers because it's quite complex. To whom do you give notice? What would be the scope of it? Would it concern all the information, or only where there's a significant risk? Who will bear the cost of that?

[*English*]

The Chair: Merci, Madame Lavallée.

Before we go to Mr. Martin, could you give us—or if not now, could you send to us—the exact section of the Privacy Act that are you are suggesting we import to PIPEDA?

Ms. Jennifer Stoddart: Yes, Mr. Chairman.

The Chair: Thank you.

Mr. Martin.

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

Ms. Stoddart, good afternoon.

I would like to jump right to the paragraph in your document from July that you circulated for comment, dealing with the fact that—and I'm actually quoting from your document—"By the end of 2005, roughly half of U.S. states had passed laws" making notification mandatory if your personal information is compromised. I'm most interested in that. I'm wondering what your current views are and if that is something you would strongly recommend the committee look at—mandatory notification.

Ms. Jennifer Stoddart: Yes, Mr. Chairman, this is something that we suggest the committee add to the act. This has become an important problem. It's become, we think, a source for identity theft, although there hasn't been a lot of work done linking identity theft to the data spills, but it must contribute to it.

We would suggest that you recommend there be a breach notification provision in this law. However, the exact wording of the breach notification is, honestly, quite a challenge. We looked at almost all of the American models, and there are quite a few variations on it.

Mr. Pat Martin: Do you think it should be graded on how serious the breach was? For instance, I've heard that one of the credit card companies, which I won't mention for commercial interests, had over three million breaches or compromises that they haven't notified their clients about. But some of those may be a matter of pennies and they were quickly corrected. Would you try to gradate the severity of the incident as to what would have to be reported?

Ms. Jennifer Stoddart: I would think you'd want to put in some criterion like "significant". You can have a technical breach of personal information, but if it's not significant, then you get into a company having to notify millions of people, which is extremely costly from the company's point of view.

Mr. Pat Martin: By the same token, those millions of people have a right to know if the credit card they're using is being regularly and frequently compromised.

Ms. Jennifer Stoddart: That is.... But if it's not necessarily significant—and then, as I say, it's not clear the exact links between breach notification and identity theft. In fact, I haven't seen any studies. Perhaps some of your other witnesses will know about that. So you can't say that because of this breach, we know that these numbers of people whose—

I think there are some states whose models seem to us more workable. We could come back at the end of your hearings and see which are the better ones.

I don't know if the assistant commissioner has any comments on this.

Ms. Heather Black (Assistant Commissioner (PIPEDA), Office of the Privacy Commissioner of Canada): It's an interesting question and something we have spent a lot of time thinking about and looking at.

On the question of credit cards, it has probably happened to you—I know it has happened to me—that I get a call from the bank saying, "Did you charge so much in a saloon in west Texas?" Gosh no, I was here in Ottawa.

It's in the interests of the credit card issuers to keep track of these things, and they do it, actually quite well, because they pay. You don't pay, they pay, because your liability is limited.

You mentioned the three million breaches. I think at one of the earlier hearings we tried to track it down and couldn't find it. It's really hard to know what kind of breach they're talking about.

● (1600)

Mr. Pat Martin: Okay, that's very helpful.

If I have a minute left, there are two other issues that have my interest—and I think I've mentioned this at other meetings too.

I know the Province of Manitoba contracted out their health data information to a private firm. That firm was then bought by an American firm, and now my personal medical records are in Dallas, Texas. God knows how many times the ownership has changed hands through corporate mergers and buyouts since then.

This has been flagged by a number of witnesses and you in your presentation, but on the cross-border jurisdictional problem of trying to protect Canadian information in other people's hands in other jurisdictions, I don't know if there are enough measures that you could possibly take to be able to give me any confidence that they're not selling my information to some drug company that's then going to use that for advertising or who knows what.

Ms. Jennifer Stoddart: Well, there are several things that can be done.

First of all, in the example the honourable member gave, I believe that is your health information that you would have given to the Manitoba government. So the Manitoba government can issue guidelines—it may have, like the federal government—and suggest that there is a scale of sensitivity. For the most sensitive things, the government may wish either its contractors to be bound by very strict contractual clauses or the data to be processed in Canada.

You'll remember the Lockheed Martin and Statistics Canada discussion of some years ago. That's in the private sector.

In the public sector, we come back to the responsibility principle I was discussing with the previous honourable member. We encourage organizations to bind those to whom they give personal information with very strict contractual clauses that allow them to do more than probably a law in the other country would, which is to go in and check, to do audits, to hold the other party responsible for damages. So I think it's quite a useful tool.

Assistant Commissioner Black has worked on some of these cases.

Ms. Heather Black: When we investigated the complaint we had about CIBC Visa, where the information does in fact flow into the United States, we discovered that CIBC had done everything they could to protect the information it dealt with. The agreement they had with the company they outsourced to dealt with safeguards, how the information could be used—as in not used, not disclosed—all that sort of thing. So they had taken all the appropriate steps, and the law in fact requires that to happen. If you're going to outsource, whether it's to the United States or to India, or wherever you're going, you are ultimately responsible. If you're ultimately responsible, you do the best you can to protect yourself as the organization in Canada so that we can't come along and say "We hold you responsible for the fact that this information was sold", or what have you.

The Chair: Thank you, Mr. Martin.

Mr. Tilson.

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

First of all, I'd like to say I'm pleased that you feel PIPEDA is working well. There are a couple of things, though, I would like to ask you about.

One of the issues that's been raised at our meetings—and we really just started and we've had two or three sessions of people coming to talk to us—is the issue of personal information, the definition of personal information in the legislation and whether or not it should exclude work product information. And you referred briefly to that in the report you made to us today, in the third paragraph on page 2. You've said that you've addressed this issue by adopting a case-by-case approach to assessing whether or not the information in question is about the individual. I gather from what you're saying that you don't believe that there should be a change in the definition, or am I misinterpreting what you're saying?

● (1605)

Ms. Jennifer Stoddart: No. Mr. Chairman, that is correct. The honourable member has exactly stated what our position is. We raise it, but our preference is that we leave PIPEDA as it is. I believe this issue was looked at in 2000. It is a flexible definition. In some of the decisions made by the Privacy Commissioner we have dealt with the issue of work product and decided that in very obvious situations it is not covered by the act, but in situations where the information is of a more personal type, more of a revealing type, the act could cover it. This is an important issue for many people. I'm concerned, Mr. Chairman, that if we go to a definition, as we go on and increasingly it's easy for employers to set up video cameras and monitor their employees in all kinds of ways, this definition will hamper our attempts to minimize workplace surveillance and to limit that kind of surveillance to what is necessary. So I think for the moment the status quo is reasonably satisfactory.

Mr. David Tilson: I guess the reason I asked that question, Madam Commissioner, is this matter did go before the Federal Court. I think it was involving a competitor challenging.... Do you know what I'm talking about?

Ms. Jennifer Stoddart: Yes, I do.

Mr. David Tilson: So one asks the question, does this give the commission too much discretion to decide on the case-by-case approach? And secondly, should the public require more certainty so that they know exactly what they should and should not do, as opposed to leaving it to the commission to decide on a case-by-case approach?

Ms. Jennifer Stoddart: My recollection of that case that went to the Federal Court was that it was discontinued. It didn't really decide the issue. I think that's something for this committee to decide.

Mr. David Tilson: Okay. Maybe when you come back you'll be able to tell us. I'm sure this topic is going to be raised in the future by individuals. I would appreciate it, if you do come back again—and I hope you do—if you would have this at the top of your list, because it seems to be one of the issues that's been dealt with.

One of the other issues is the issue of solicitor and client privilege. I'm not familiar with this case you've spoken of, this Blood Tribe case. Are you saying the commission should be allowed to go beyond solicitor and client privilege? Is that what you're saying?

Ms. Jennifer Stoddart: Yes, Mr. Chairman, that's what we're saying, and we do in the Privacy Act.

Mr. David Tilson: You see, I always thought that whether documents are solicitor and client.... Are you saying you should have the right to that information, whether there's solicitor and client privilege or not? Is that what you're saying?

Ms. Jennifer Stoddart: Yes. We're saying that in the course of our investigations we have to be able to look at all the documents that are relevant to our investigation.

Mr. David Tilson: You're going to get the law societies and the Canadian Bar Association all excited.

Ms. Jennifer Stoddart: I think they already are, Mr. Chairman. We'll worry about that later.

Mr. David Tilson: I know, and I'm sure someone will come and challenge you on that. I must say, there are a lot of lawyers in this room and I can't believe they aren't excited as well. It's quite a major —

Ms. Jennifer Stoddart: Yes, it's a fundamental issue.

Mr. David Tilson: I don't know of any situation—and if there are, there are very few of them—where you can simply go beyond solicitor-client privilege. It's quite a major statement.

Ms. Jennifer Stoddart: It is, but the first level of court agreed with us, so it's not patently unreasonable.

Mr. David Tilson: No, but the second level didn't.

Ms. Jennifer Stoddart: Well, we may take it to a third level.

Mr. David Tilson: Okay, there you go, Mr. Chairman.

With respect to your consultations on the 12 issues, you're going to give us those, are you? You mentioned 12 issues that you had. Is that somewhere in the documentation we have?

● (1610)

Ms. Jennifer Stoddart: You have a résumé of the answers that came back, the background information. It's a document that was given to this committee, some 36 pages, and you have a résumé of the positions.

Mr. David Tilson: Okay. One of the issues I'm interested in is whether PIPEDA is doing enough to facilitate small business.

Ms. Jennifer Stoddart: That's an excellent question, Mr. Chairman. Most of our complaints are against the large organizations that are the federally regulated organizations. In some provinces, of course, we don't see the small business, because it's the provincial laws that apply. Certainly when PIPEDA first came we had extensive meetings—particularly the assistant privacy commissioner responsible for PIPEDA had extensive meetings with representatives of small business. We consulted them as to what they would need. We are currently working with our enhanced budget that was granted to us, and we're working on an interactive tool for businesses for implementation of PIPEDA, with small businesses in mind that don't have a lot of money to invest in privacy compliance.

So the short answer is you're probably right that we're not doing enough, but we're trying to do more.

Mr. David Tilson: No, I didn't say that. I was simply asking whether you were or not. I guess now that you've said that you're probably not, can the legislation be changed to assist small business more?

Ms. Jennifer Stoddart: I wasn't thinking of that, Mr. Chairman. I was thinking that the burden of compliance generally tends to fall quite harshly on small businesses. In that sense, it's my own personal opinion that I think we may not be doing enough.

I mentioned this interactive video that would be a learning tool. It is designed for small businesses that don't have the money to go out and hire privacy consultants and so on, the way the big businesses do.

The Chair: Thank you.

Before we go on to our next round, simply to be crystal clear on your position with respect to solicitor-client privilege, in your opening remarks you said, and I'm quoting you,

> It effectively allows organizations to shield information from our investigators with no independent verification that the documents in question do in fact contain information subject to solicitor-client privilege.

There's a major difference between saying we should be able to look at the documents to determine whether or not they are subject to solicitor and client privilege, and saying we should have access to all documents, even those that are subject to solicitor and client privilege. Do you understand the difference of what I'm pointing out? If so, which is your position?

Ms. Jennifer Stoddart: I think it would involve both. Our position is that we should be able to look at the documents to see if they would be subject to a solicitor-client privilege, and if not, to examine them to see if they have personal information relevant to the investigation.

The Chair: Clearly. But if so, what if your investigation finds that they are subject to solicitor and client privilege?

Ms. Jennifer Stoddart: Then I think that would be it.

The Chair: We'll get to that.

Go ahead, Ms. Black.

Ms. Heather Black: To put this in context, to take the fact situation in the Blood Tribe case, our complaint came from an employee of the Blood Tribe. Blood Tribe is a federal work under the definition, so we investigated. She wanted access to her personal information held by her employer, and the employer said you can have this, and you can have this, and you can have that, but you can't have.... It was a few documents that they claimed were privileged.

In order for the commissioner to do her job and say "You correctly invoked this exemption to disclosure because you don't have to disclose to your employee a privileged document", we have to be able to go in there and look at that document and say "Yes, it is privileged, and you're right, you don't have to disclose it to the complainant". That's the sort of situation we're looking at. It doesn't come up in every case. In fact, it rarely comes up. It's very rare that an organization actually claims the exemption for solicitor-client privilege when faced with an access request.

● (1615)

The Chair: I guess what you're basically saying is there should be some mechanism to determine whether or not the claim of solicitor-client privilege is in fact a valid claim.

Ms. Heather Black: That's right.

The Chair: Thank you.

Mr. Dhaliwal, please, for five minutes.

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

Marlene, do you want to go ahead or do you want me to go ahead?

Hon. Marlene Jennings (Notre-Dame-de-Grâce—Lachine, Lib.): If you have questions, go ahead. If not, I have questions ready.

Mr. Sukh Dhaliwal: I'll pass it on to you, then, for my time.

Hon. Marlene Jennings: Thank you, Chair, and thank you, Mr. Dhaliwal.

Thank you very much for your presentation. I apologize for missing the first part of it. I had not received the information that the committee room had changed, so I was at 371 West Block.

I'd like to ask you about three issues. I'll try to be very brief in my questions, and if you don't have enough time to respond fully, you know the routine, that you can send it on in writing.

On the question of the obligation of notification when personal information held by a company—for instance, a credit card company or a bank—has been either lost or stolen, there's a whole issue about the need to have a mandatory requirement to inform the individuals that their personal information has been violated, and that at this point in time you, as commissioner, have no way to penalize companies that do not notify.

If you're seeking authority to be able to compel companies that hold personal information legally, but from whom illegal access to that personal information has been gained.... You're seeking the authority both to require the company to inform the individuals whose personal information has been violated and to penalize the company that does not do that. Does that not accord better with the model of a commissioner who has the power to issue executive orders, rather than an ombudsman model?

Secondly, on the issue of work product, I liked the point that Mr. Tilson raised. Notwithstanding that you would prefer to continue on a case-by-case model or process of dealing with the issue of whether the personal information is worthy of privacy or whether it is work product, I think there is a compelling need. There are companies that deal with personal information, and if we want to ensure that the processes that they put into place are in fact well founded and they're not going to suddenly be caught up short after possibly months and thousands and in some cases millions of dollars invested into putting into place the process in order to legally capture personal information, treat it, send it out legally, and all of that, and then all of a sudden there's a decision that says “Oh no, that's wrong, you can't do that with that information or parts of it”.... If there were a distinction between personal information that comes under privacy and under work product, with whatever clarifications are needed to ensure that the scope is not too large, is sufficiently narrow, but is very clear, I think there's a good argument for that. Professor Bennett, who came before the committee, also was in favour of it, as was the other professor who was here.

My third question is again on the issue of the ombudsman model. You have no executory powers. There are models that are not quite ombudsman—it's a mixture—and there is the authority and there is a way to build deadlines and delays into legislation in order to ensure that the process for handling the complaints and disposing of them can be done in a very fulsome manner, but very efficiently and quickly, rather than a year or two years, etc.

If you're not prepared at this time, I'd like you to reflect on that. I think the models in British Columbia and Alberta have provided sufficient information to allow us to move forward.

● (1620)

The Chair: For the guidance of members, that took four minutes and 45 seconds.

Hon. Marlene Jennings: And you're welcome, sir.

The Chair: Could you please, Commissioner, either give us a very brief response to those three questions or perhaps a written response later? Do you have any comment on any of the three?

Ms. Jennifer Stoddart: Yes. What would be most useful to the committee?

The Chair: Whatever you'd like.

Ms. Jennifer Stoddart: Could I do both, Mr. Chairman?

Very briefly, to the honourable member, we forget that in the current model the Privacy Commissioner has a whole series of powers. We forget because they were not used in a consistent way from the beginning. We are now taking cases to the Federal Court and are involved in 12 cases. We have an almost total rate of compliance when we say we're going to take cases to the Federal Court.

The Federal Court, remember, can order damages. None of the provincial commissions can order damages. You can make an order —it's the same as our recommendation—and it's a binding order, but it doesn't really put the person in the place they would have been had there not been a privacy breach, because it can't account for damages. I think that's an important issue.

The Chair: I think I'll stop you there, Commissioner, if you wouldn't mind. If you could provide written answers to the other two, thank you.

Ms. Jennifer Stoddart: Okay, certainly.

The Chair: Mr. Wallace.

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

I'll ask questions and give you a chance to answer.

It's come to my attention that there are organizations who like the B.C. definition. Do you want to comment on the British Columbia work product?

Ms. Jennifer Stoddart: Certainly. I think the B.C. definition, as I understand it, is well received in B.C.—and I think you may have the commissioner here to comment on that.

I will simply reiterate, from the point of view of the protection of privacy, that when you go for any definition of work product, it may have the effect of narrowing the protections for other related information related to a person's employment.

Secondly, I note that the B.C. definition does not provide for consultation. In fact, as I remember, it excludes the work product from the definition of personal information.

Another provincial jurisdiction has in fact put in a step of consultation with those whose personal information is being collected. I think that's an interesting facet that is not in the B.C. legislation.

Mr. Mike Wallace: Okay, I appreciate that.

I'm going to follow up on my colleague's question about the private sector piece. Because I'm new to this issue and didn't have the experience of working for a company related to this, what is the average cost of this program for a small business? I know you said that with your increased budget you're looking at ways to better communicate to organizations how to implement PIPEDA, but what are the costs to small and medium-sized business, if you have a sense of what those are? And do you care?

Ms. Jennifer Stoddart: Yes, I certainly care. I care that the law is as easy to apply as possible, because privacy is a fundamental right in this country and Parliament has adopted this law. I care about whether it is practical and easy to apply.

Mr. Chairman, the assistant commissioner deals very closely with a lot of these cases, but if I may, before I ask her to give some examples of how small business tries to comply, I'll just say that Parliament, as I understand, deliberately chose a very light and flexible regulatory system in 2000. I'm saying this to the honourable member because it could have chosen a much heavier system—for example, the British system, where you have to register your databases with the U.K. commissioner every year and then pay a registration fee. That's how the U.K. commissioner in fact finances his office.

But here in Canada we just said this is the law and you're expected to comply with it, and unless there is a complaint, or the Privacy Commission does an audit or something like that, we will presume—as with most of the laws of this country—you are in compliance with it. So it was supposed to be a light law.

● (1625)

Ms. Heather Black: As you probably know, the law is based on the CSA model code for the protection of personal information, which was developed as a voluntary instrument by various stakeholders, including business.

It's a management standard, so it's quite easy to apply. It wasn't developed as a law for big business or little business; it works for everybody. If you're a small business, your privacy policy can be one page. If you're a huge organization, your privacy policy is probably thicker than this binder. It's that sort of thing. So it's not difficult for small business to comply with the law. A lot of them are trying to comply, and I think part of where we could possibly do a bit better is in education and in working with small business.

Mr. Mike Wallace: And during your budget consultations here a few weeks ago, that was part of the process. That extra money was to help promote PIPEDA on how to get up to speed on that. Is that an accurate statement?

Ms. Jennifer Stoddart: Yes.

Mr. Mike Wallace: And when would we expect that to be available to the public?

Ms. Jennifer Stoddart: In the course of this winter, I think, Mr. Chairman.

Mr. Mike Wallace: Okay, thank you, Mr. Chairman.

The Chair: Thank you.

Monsieur Laforest.

[*Translation*]

Mr. Jean-Yves Laforest (Saint-Maurice—Champlain, BQ): Good afternoon, madam, and welcome.

Toward the end of your presentation, you told us that it was possible to improve the act and you made a few suggestions. However, some witnesses have told us that the fact that your office or you yourself don't have the power to make orders slightly complicates the process for them following an investigation.

When you compare that somewhat with the power that the commissioners have in Alberta and British Columbia, this is a process that could help. You said that you didn't intend to seek additional powers. I have trouble understanding why you say the time isn't right.

Is it only the time that isn't right?

Ms. Jennifer Stoddart: You referred to Alberta and British Columbia, but that's also the case in Quebec.

To answer your question, I'd say that the time is very important. I believe we haven't really had the opportunity to implement this act as we should have done, let's say, until April 1 of this year, when we had granted a budget commensurate with our tasks and had an office stable enough and an implementation plan that had been thought out in advance, that was coherent and that reflected the needs of both parties, etc. Before, it was somewhat erratic. This is an office that has experienced a number of disruptions.

That said, we have extremely broad powers. I told your colleagues that, with one exception, all the businesses that we told that we didn't agree with their interpretation of the act, that we believed that the complaint was founded and that they should take this or that remedial measure, reacted well. When we said that we wanted to go to court and that a Federal Court judge would make a decision, all those businesses complied with our requests, except one, for the moment, and we haven't thoroughly argued the case.

I also have a power to conduct audits. As you've no doubt seen in the papers, one company is disputing our power to conduct audits through the judicial review process. This is an enormous power. We can seek remedies for damages, and we can seek remedial measures.

Mr. Jean-Yves Laforest: You can seek?

Ms. Jennifer Stoddart: We can seek remedial measures before the Federal Court.

Mr. Jean-Yves Laforest: Does that become binding?

Ms. Jennifer Stoddart: Yes, in a Federal Court judgment.

The purpose of the act is to settle complaints. I think the purpose of an act isn't, in itself, to make orders. The purpose of the act and of the machinery that administers it is to ensure compliance. If you take a close look — which few people have done — at current compliance with this act regarding the complaints process, you'll see that it's very great, except for a few judgments such as in the Blood Tribe judgment, for example.

I don't think the problem is the way complaints are handled. I don't think it's less efficient than what you see before the courts. I administered a tribunal in Quebec, so I think I'm talking in full knowledge of the facts. Before the courts, there may be enormous legal complications. It's not as quick as we'd like. The problem isn't the handling of complaints received. The problem is everything that happens that isn't subject to a complaint. I think that's the major issue.

● (1630)

Mr. Jean-Yves Laforest: So the fact that you don't necessarily want new powers immediately in this regard isn't just attributable to the time, which, as you say must be considered as important. It's also very much a matter of substance because, ultimately, you're saying that you think the powers you already have are quite sufficient. Later, you might possibly see whether other powers would be necessary.

Ms. Jennifer Stoddart: That's correct. I think I have broad enough powers. I haven't had the time... I haven't been commissioner for a long time, and you know that the first years of my term were devoted to restoring the office, but I have very great powers under this act. Give me a little more time to exercise them, and you'll see in five years whether that was effective or not.

Mr. Jean-Yves Laforest: That's perfect. That's a very good answer to my questions. Thank you.

[*English*]

The Chair: Merci, monsieur.

Mr. Van Kesteren is next.

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

Thank you for coming here again.

I've got to say that when you and I first spoke about your job, Madam Commissioner, it certainly was an enlightenment on a personal basis, because I was the owner of a small business prior to this, and I've got to tell you that it struck terror into all our hearts when the mandate came down.

When I listen to the testimony, it appears to me that you don't really have a heavy-handed approach unless there's cause or unless there's violation. Am I correct in assuming that?

Ms. Jennifer Stoddart: Yes. The law is flexible. It's a fairly light law, but if there is a complaint, we investigate that complaint until there is a settlement or we say it's not founded. We're not letting people at this point just.... We're not saying it's well founded and then walking away. Sometimes I read that the Privacy Commissioner said something is well founded, and then nothing happens. Well, that may have been true in the past; for over a year now, if it's well founded, then we are ready to go to court to hold up our interpretation of the law. We've had virtually total compliance on this—but it's very few cases, honourable member, so in that sense, it's—

Mr. Dave Van Kesteren: Somebody has to initiate a complaint, first of all.

Ms. Jennifer Stoddart: That's right.

Mr. Dave Van Kesteren: I think my colleague was alluding to that in his prior question.

As you move forward, have you thought about portraying that message? Again, I'm thinking about the small business person looking at the mountain of paperwork and these new tasks being put in front of him. Maybe we could convey to him that this is what we don't want you to do—you've got to fall into these guidelines so that you don't break the law, you don't offend and, as somebody said, violate somebody's privacy. Is that something you're possibly going to consider at the next stage, so that the smaller business owner understands? I really don't think they understood, as I didn't, the true nature of the legislation.

Ms. Jennifer Stoddart: Yes, Mr. Chairman, the honourable member is completely right. On January 1, 2004, some amazing misinterpretations of PIPEDA were circulating, and I think there was a sense of panic. Of course, a lot of that was the fact that the office had been in such upheaval and hadn't done what ideally it would have done, although it did consult with small business.

Yes, we have identified small business as a very important target for public education. I must say that I don't think a heavy hand should be brought to small business on this kind of issue. We have major players; most of our personal information is with the major players in this organization. I would certainly concentrate my attention on them first.

Mr. Dave Van Kesteren: As I said, once the objective was made clear, then it all made sense. I think most people would fall into the same category I was in.

Do you have inspectors out in the field and checking for compliance?

● (1635)

Ms. Jennifer Stoddart: No, we don't have inspectors. We have auditors—

Mr. Dave Van Kesteren: You have auditors.

Ms. Jennifer Stoddart: —but we have to have reasonable grounds to believe there's a problem; we have to have noticed something. We have two cases in which we've sent in our auditors, but this was not small business, I may say.

Mr. Dave Van Kesteren: Probably the biggest concern—and I think Mr. Martin alluded to that as well—occurs when a corporation is in a takeover, and that crosses borders. When you have those takeovers and you really don't know what's going to happen to that information, is that your biggest area of concern?

Ms. Jennifer Stoddart: That has to do with being able to share personal information in the case of a sale. Is that what you're referring to?

Mr. Dave Van Kesteren: Any information, anything that could be used, like Mr. Martin said, for your health.... If, for instance, you had to buy life insurance and my life insurance company was transferred to another country, they could make it difficult for me to buy auto insurance or something like that. Is that an area of concern?

Ms. Jennifer Stoddart: Yes. Perhaps it's the same issue the assistant commissioner was giving some examples of. We then may require of those companies that may be sending your information outside the country that they hold those to whom they are sending it to Canadian standards so that this would not affect you in any more negative a way than were it completely treated in Canada.

Mr. Dave Van Kesteren: You have jurisdiction over those companies if they are outside of our borders?

Ms. Jennifer Stoddart: No. This is the hook and this is the interesting part of it. Through this mechanism, we have jurisdiction over the Canadian companies because it has a presence or a real and substantial link as the legal test in Canada. As you know, in the privacy world there are some countries that say their legislation has an extra-territorial reach, and on the other hand, Canadian law doesn't usually run except in Canada, and so on. The surest thing is the companies here are responsible for how they send the information out.

Mr. Dave Van Kesteren: Thank you.

The Chair: We have Mr. Martin, followed by Mr. Dhaliwal and Mr. Tilson.

Mr. Martin.

Mr. Pat Martin: Thank you, Chair.

I was just reading a letter from the Assistant Deputy Minister of Industry pointing out that an organization in the U.K. ranked Canada's privacy regime as tied with Germany as the best in the world. I think that's something to be proud of. In contrast to that, or building off that point, I'm horrified at what I'm learning now as to what might be the real threats to privacy and the next generation of privacy issues, specifically the RFID information.

I only heard of this in the last few months. I don't think Canadians are aware of the idea that you can implant a chip in cards or in people and read it quite easily from a distance. Somebody asked how you would feel if the underwear you were wearing was helping to track your movements around the city. That's not inconceivable with this technology.

I'd ask you to speak to that and what your office is aware of, and what you can recommend to us to get on top of that next generation of technology. Is there any funded research going on, sponsored by the OPC on our RFID, and if not, should we not perhaps think of that?

Ms. Jennifer Stoddart: Yes. Could I ask the assistant commissioner to speak to the research that was done a couple of years ago?

Mr. Pat Martin: Certainly.

Ms. Heather Black: I don't have the details at my fingertips, but yes, we did fund one of the universities. I think it was the Dalhousie Law School in conjunction with their computer engineering school. They came forward with a project on studying RFID.

● (1640)

Mr. Pat Martin: What's the status of that study? Do you know, Ms. Black? Is it under way?

Ms. Heather Black: Oh no, it's completed. They did provide us with a paper on it.

Mr. Pat Martin: Perhaps you could circulate that to the committee.

Ms. Heather Black: Absolutely.

Mr. Pat Martin: I'd be very interested.

Ms. Heather Black: There is a fair amount of not so much disinformation as fear out there about RFIDs and what they're capable of doing. Right now there's limited use of them, but you're right, there's a whole great new world of RFIDs on its way in things like credit cards. There are some astounding instances. Apparently there was a bar in Barcelona, Spain, for example, that—

An RFID can be the size of a grain of rice, and you can have it embedded under your skin. It's scary to some of us, and other people say “Gee, what a great idea, because I don't have to carry my wallet and my ID and all that stuff. They scan it when I get a drink or whatever.” You have to face the issue that people are often willing to sacrifice a fair amount of privacy for convenience.

RFIDs in credit cards, for example, will probably bring us a new level of security with credit cards. They'll be maybe chip-enabled and have passwords and stuff like that.

We are working on RFID guidelines, which will be posted, I believe, on our website fairly soon, sometime this winter. There is information on RFIDs on the website of the Information and Privacy Commissioner of Ontario. There's a fair amount of information out there, but we will provide you with whatever we can.

Mr. Pat Martin: Great. Thank you.

The Chair: This hearing is being televised, and hopefully there will be some people who look at it. They may not know what an RFID is. Would you help them out?

Ms. Heather Black: An RFID is a radio frequency identification device. There are two types: active and passive. Some can only be read when they're put near a reader, and some actually emit a little signal.

I don't know if you buy books at Chapters, but occasionally a little square piece of paper will fall out of a Chapters book, and it has a little design thing in it. That's an RFID. If you fly via the airport in Hong Kong, your luggage is tracked by an RFID. They stick it on your luggage and they can track it through the airport. It's being used a lot at the wholesale level to track shipments of goods from the factory to the distributor.

The Chair: Thank you very much.

We will go to Mr. Dhaliwal.

Mr. Sukh Dhaliwal: Thank you, Mr. Chair.

Thank you, Madam Commissioner and Assistant Commissioner.

This work product issue has come up again and again in these proceedings. Could you clearly explain the difference between work product and personal information when it comes to the medical field?

Ms. Jennifer Stoddart: In the medical field?

Mr. Sukh Dhaliwal: I mean in medical records.

Ms. Jennifer Stoddart: Well, personal information in medical records, let's say, would be the contents of my file, the medical details about me: my state of health, the results of my latest tests, things like these. This is all personal information related to me.

In the case where the Privacy Commissioner decided that some alleged personal information was in fact a work product, as I remember it had to with the prescribing patterns of doctors. So it wasn't personally about the doctor—himself or herself—like the contents of my medical file would be about me. Rather, it was the information about the doctor displayed through his or her professional activity.

Mr. Sukh Dhaliwal: So you would call it a work-related product, then. Right?

● (1645)

Ms. Jennifer Stoddart: It was decided that it was not personal information.

Mr. Sukh Dhaliwal: Would you have any difficulty, then, incorporating that into PIPEDA?

Ms. Jennifer Stoddart: As I said, it's always easier to define things in a particular fact context. You mentioned that this issue came up again and again. It doesn't come up very often in our complaints. I don't know how many complaints we've had that would deal with that—perhaps a handful. This is not an issue that dominates our complaints.

One issue that does come up a lot in our complaints, and one area where we have active concern, is about the use RFIDs or other ways of surveilling people in workplace surveillance. Those of us who work for anybody are going to be subjected to increasing surveillance.

So yes, you could put a definition in the act. We're just cautioning you that any definition may have this indirect effect, with new forms of technological surveillance coming, of providing less protection for workers.

The Chair: I wonder if you'd be kind enough, Commissioner, when you come back, to give us a concrete example of what you're talking about. I'm having a great deal of difficulty making the leap between what Mr. Dhaliwal was talking about—the prescribing habits of doctors—and how, if there were a definition in the act, that would somehow impact on the privacy of employees in a washroom in a factory. Perhaps you could help us out by giving us some concrete example of how the one follows the other.

While it may not be a major one of the 1,400 complaints you've received, it has been brought up by virtually every witness, and I believe it will be brought up by other witnesses. Clearly it's of some concern to some businesses out there, and they'll be looking to us to make some kind of recommendation. If you could help me and the committee with how you figure the one has anything to do with the other, that would be a great service to us.

Mr. Dhaliwal.

Mr. Sukh Dhaliwal: Further, Chair, most of that information these days is used for research and development purposes.

Take the information on, for example, the prescribing pattern of doctors, how they prescribe medicine. If the information is used for research purposes, would it still fall under personal information? If it's for business purposes, would it fall under PIPEDA?

Ms. Jennifer Stoddart: It's at the time the information is generated with the organizations that it's qualified. It's the circumstance in which it's generated that leads to the definition. Afterwards, for example, it may be anonymized, and then it isn't personal information for various points.

We'll come up with an example, Mr. Chair.

The Chair: Thank you very much.

On that point, you mentioned that the Privacy Commissioner had made a ruling. Are you bound by that ruling? As the new Privacy Commissioner, could you change it? And even if you confirmed it, it's my understanding that it's not binding on the Federal Court, whereas a definition in statute clearly would be.

Ms. Jennifer Stoddart: You're right that the ombudsman's conclusions are not binding on Federal Court. Certainly as an ombudsman one has a certain amount of latitude in conclusions, but as I think one of the honourable members said, it's always a good idea to provide predictability. We try as much as possible to provide a continuous line of reasoning in our conclusions.

The Chair: Just to be clear, you could overrule a previous commissioner if you so chose.

Ms. Jennifer Stoddart: Technically, yes, I could. It's not binding, really, on anybody. It's an opinion.

The Chair: Right. Thank you.

Mr. Tilson.

Mr. David Tilson: Thank you, Mr. Chairman.

One of my colleagues, I think Madame Lavallée, asked a question on the issue of transferring a file to another jurisdiction. Your response was that you could indeed transfer a file to another jurisdiction.

I'd like you to talk a little bit about that. Are you telling me that you could conceivably transfer a file to one of the European states, or to the United States? Is that what you meant by that?

● (1650)

Ms. Jennifer Stoddart: Do you mean that I could, as Privacy Commissioner?

Mr. David Tilson: Yes.

Ms. Jennifer Stoddart: No, I don't think I can now.

Mr. David Tilson: You'd be breaking your own law.

Ms. Jennifer Stoddart: Well, that's what we think, although in the consultation, it's interesting that many people responded that the Privacy Commissioner should do whatever is in the public interest, and they would take a generous view of this.

I don't see that it's clear in the law, and in fact, I would think the law says the contrary: that I can't transfer a file to the EU, for example.

I'm saying that in the state of the world, I think I should be able to, if the circumstance warrants it. The Federal Trade Commission is currently asking for the same kind of powers, because it's very hard to follow the data trail now.

Mr. David Tilson: Would you have a definition as to the circumstances in which you would do that? It gets back to the issue of the earlier question I asked on personal information. In other words, you look at everything on a case by case basis. I suppose the same would apply, and you'd look case by case at situations as to whether or not you could transfer a file to another jurisdiction.

I would think that, to serve the best interests of the country, we'd want a specific definition, if you were to do it. Quite frankly, I don't see how you could do it, because you'd be breaking the law.

Ms. Jennifer Stoddart: I don't do it, honourable member.

Mr. David Tilson: I must have misinterpreted what you said. You thought there might be circumstances when you could transfer a file?

Ms. Jennifer Stoddart: Perhaps I wasn't clear. There may be circumstances—in fact, one could think now that there are circumstances—where it would be very useful for me, as Privacy Commissioner, to be able to transfer a file to a similar organization in another jurisdiction under wording—because you asked for wording, honourable member—something like "for a complete and satisfactory resolution of the case", with the consent of the individual, of course.

If I said, basically, "You've been a victim of some organizations in the United States", and I'll use some cases that are well known, and in fact part of this is before the Federal Court, "but in order to really get some redress, it would be better if the American authorities took up your case", as police investigators do—they'll transfer it and go after it under their own laws—the Americans then could go—

Mr. David Tilson: Except that we're all very proud of our own sovereignty, our own jurisdiction, and not assigning our laws to any other country, or our proposals, whether it be in privacy or police work; we're going to look after—

Ms. Jennifer Stoddart: We are very proud of it, but that pride does not give us the legal right to, for example, investigate in the United States or act as the police. It's in cases where I couldn't act, which is in most other jurisdictions. I would say, could you take this over? And vice versa, if they had somebody who was coming against their personal information, they would transfer it to me.

Data protection authorities across the world are looking at this. Some European ones already have the powers, because they're in closer contact than we are. The Federal Trade Commission has a series of amendments before Congress called the SAFE WEB Act that would allow them to do that for those reasons, because Americans' information is everywhere.

Mr. David Tilson: Mr. Chairman, I have a question with respect to electronic payment crime, which is on the increase. In 2004 the federal government announced the creation of something called the "cyber services task force". Do you know what that is?

Ms. Jennifer Stoddart: No.

Mr. David Tilson: Okay, we'll move on to something else.

Ms. Jennifer Stoddart: There is an anti-spam task force, but—

The Chair: You're at five minutes.

Madam Commissioner, to follow up on Mr. Tilson, you said: "I would ask you to consider a specific provision to make it clearer we"—I presume the commissioner—"have the authority to share information with our international counterparts while cooperating on investigations of mutual interest".

That's what you're asking for, to share information. Is personal information of Canadians what you mean? And you want to be able to share it with international counterparts? Am I reading that correctly?

● (1655)

Ms. Jennifer Stoddart: Yes. And I would like to share it not only on cases that are of mutual interest, but on cases where it would be in the interest of Canadians that the investigation of the redress be followed up in another jurisdiction.

The Chair: Madame Jennings.

Hon. Marlene Jennings: Thank you.

I'd like to come back to the question that my colleague Mr. Dhaliwal raised about aggregated prescribing information and the possible necessity for a carve-out and a clearly defined exemption.

Due to medical advances we have an increasing number of drug therapies to treat all kinds of health conditions. We have medical practitioners who require scientific information about the impact of certain prescribing profiles. We have researchers who also require this kind of information.

Do you not think it is possible to do a very clear carve-out that would provide an exemption for aggregated prescribing information that would not affect the fears you have of weakening privacy protection for personal information if a definition of "work product " is done, because that would make it so large as to weaken that protection? Is that something you think could be considered?

Ms. Jennifer Stoddart: If the honourable member has a specific type of work product information in mind, it would doubtless be possible. I was replying in a generic way for all kinds of work product information. I believe you mentioned prescription patterns. That could probably—I'm saying probably because I haven't done the exercise—be specifically carved out. Then it would be fairly clear that it wouldn't spill over into the other issues of workplace surveillance that I'm concerned about.

Hon. Marlene Jennings: Thank you. I would appreciate it if you would look at that and possibly propose an actual carve-out for that specific type of work product information. But it would be specifically aggregated prescribing information.

The other point I want to get back to is the CSA standard as a model. We've heard from expert witnesses that it's actually a good model because it's a fairly light-handed model that provides a building block from the bottom up. However, when we come to the issue of consent and the definition of consent, studies have shown that a significant number of companies imply consent, and the way they obtain consent may not be as clear to the consumer as one would hope. These organizations are recommending that the whole issue of consent be tightened up so it has to be a proactive thing, rather than implied.

I'll give you an example. I received in the mail an application for a credit card saying I had been pre-approved for a $25,000 credit limit—simply sign it off. But there was a whole section on privacy. I scratched it out and wrote by hand that I consented to the use of my personal information solely for the purpose of obtaining the credit card. I did it as an exercise.

The company sent me back an application three times. So it was clear that they wanted to use my information for more than just issuing me a credit card. That's implied consent. I think it should be tightened up, but I'd like to hear from you on that.

Ms. Jennifer Stoddart: Consent, of course, is at the heart of the protection of privacy. As you say, the problem of tightening it up goes to the challenge of trying to provide a basic definition of all the contexts in which you give consent. That would be quite a challenge, and I would not be able to suggest how you would say in such and such situations it's expressed consent and in other situations and so on. In enumerating them, we have provided guidance, we have suggested the level of consent. We have many conclusions on this, that the more sensitive the information, the more express the consent would be. We've gone into the issues of what a reasonable person would consider appropriate in consent in the circumstances.

It is not an issue for the law to be tightened up, but for compliance work. This can be. If you had made a complaint, for example, that would have allowed us to go into the current practice. Why is that company coming back again and again? We may have seen them already, or we have never seen them. It would be a chance, an open door, but everybody doesn't have time to make complaints to the Privacy Commissioner; that's the problem.

● (1700)

Hon. Marlene Jennings: Next time I get that and I cross it out and put my express and limited consent, if I get another application, I'll send it to you with a complaint.

Ms. Jennifer Stoddart: Okay. We'd be happy to have it. Because one thing we have done, as I remember—I think the assistant commissioner remembers the details of this—is we have said very clearly to organizations that when consumers say no, they don't want to receive things and they don't want to be on mailing lists, you have to respect their wishes. You can't go on and on and batter them into finally receiving the material you want them to.

I don't know if you want to hear about those cases. We had several cases on that.

Ms. Heather Black: As you know, the code says specifically that you can object to the collection, use, or disclosure of any personal information that's not required to provide you with the service. In the case of the credit card, what information do they need, how do they need to use it, to whom does it need to be disclosed to provide you with the credit card? When it goes beyond that, when they say when you sign up here we're going to market you, or we're going to release your name to third parties they think you might want to hear from, maybe I don't want to hear from them.

It is covered in the law, so it's a question of educating organizations. And the thing they need to be reminded of constantly is listen to your customer. What does your customer want?

The Chair: Thank you.

Ms. Yelich.

Mrs. Lynne Yelich (Blackstrap, CPC): My concern as a consumer or as a client is that I wonder what I'm signing, what authority I'm giving to people. For instance, the dentist wanted me to sign something. They just said sign here, it's really nothing, just this new Privacy Act that's out there. I said I didn't mind signing it but asked what they were going to do with the information. I don't care if I get extra mail; that isn't what's bothering me. But what are they going to do with it?

So I wonder how much I am giving them, and you've more or less answered that. I still don't know. I guess it's the individual circumstance.

You said there were 56,000 complaints and inquiries. What's the background of those? Is there a certain sector that has more inquiries in your office than others? I just want to get into perspective what it is that your office is really addressing.

Thirdly, because I don't want to come back, in my riding I had a car dealership that immediately was very upset. Everybody thinks car dealers are rich, but they find it difficult because these people have to hire somebody else to do the databasing. Maybe they're overreacting, which is going to be my question. Are they overreacting? They want to database not only the customer, but whether that customer chose a particular colour of car or if they took it for a test drive. They're trying to database all of that information. Perhaps their dealership is overreacting, so I just want to know if it's something that sounds unreasonable when they say they have to hire somebody just to database all this extra information that they require from a customer. Of course, when you're dealing with cars, you probably are trying to get them on a mailing list to entice them to buy cars.

● (1705)

Ms. Heather Black: Maybe they're overcollecting.

Mrs. Lynne Yelich: I would say they are, but this was actually a directive from their parent company. So I just wondered about that. I actually had a letter from them—perhaps I should get that letter to you—describing just how cumbersome it was and the fact they had to protect themselves. That's how paranoid they are.

I think you're right. The level of communication is quite low in terms of understanding what you have to do to protect yourself from anyone who might take you to court.

So to go back to the 56,000, I'm just curious, and then I will—

Ms. Jennifer Stoddart: I don't have the breakdown here about those inquiries—

Mrs. Lynne Yelich: Just ballpark.

Ms. Jennifer Stoddart: —but most of the complaints are against financial institutions, because they are regulated by the federal government. How many bank accounts do we all have on average? The number is probably four or five per Canadian. There are all the mortgages and all the amounts of personal information that go around financial institutions, including credit card companies. That is the first major sector.

We then have insurance companies, again because they handle a lot of personal information. We have transportation, because the federal government regulates transportation. In particular, airline transportation requires a lot of personal information. And there's telecommunications. Once again, that brings us into phone companies and cable companies and so on, which again are increasingly linked up with other suppliers. That's basically the picture.

Mrs. Lynne Yelich: Thank you very much.

I want to go back to my first question. Is there such a thing as reverse onus or burden of proof? If I signed something and then found out I wasn't happy that they used my name in something, could I lay a charge against that company if I really didn't think they.... Would the burden of proof lie with me?

Ms. Jennifer Stoddart: In making a complaint, yes. I would say you can, but I'll let the assistant commissioner explain.

Ms. Heather Black: If you've signed something and then you change your mind, you have the right to withdraw your consent.

Mrs. Lynne Yelich: You have to do it that way.

Ms. Heather Black: Quite often, organizations don't listen to someone who tries to withdraw consent. They may explain to you that they can no longer provide you with the service if you withdraw consent, but in a lot of cases—say, for third-party marketing or something like that—you can withdraw your consent, and if they don't listen to you, then by all means complain.

Mrs. Lynne Yelich: I was just wondering, because sometimes you don't know what you've signed until the basics of it come to mind.

Thank you very much.

The Chair: I have just a couple of questions, if I may.

One of the roles of the Privacy Commissioner under PIPEDA is education and information, as it is under the Privacy Act. I heard a startling statement at last Wednesday's meeting made by Mr. Richard Rosenberg, president of the British Columbia Freedom of Information and Privacy Association. I want to quote it for you and ask for your comments:

> Second, a much more effective education function is required. The OPC could serve a more effective role than it has up to now; namely, to bring the office and its role under PIPEDA to the attention of the Canadian public. In my classes and talks I have rarely found anyone who knows about Canada's privacy law, his or her rights under the law, or the existence of the OPC, the current Privacy Commissioner, or the activities of the office. A survey commissioned by the Office of the Privacy Commissioner in March of this year showed that something like 8% of Canadians had heard of PIPEDA. Clearly, if you're not aware of laws protecting you, it's going to be hard to take advantage of the protection they provide.

I'd like to give you the opportunity to respond.

Ms. Jennifer Stoddart: Thank you very much, Mr. Chairman.

You may remember that in the submission we made last fall to the special parliamentary review panel, and we met with your committee two weeks ago on our budget, a good part of the increase in the budget was because we realized that we were not resourced and able to meet the public education challenge. We have been since April 1. I gave you some examples of the increase, then, in our outreach and our visibility, notably through the media and through the website.

For the past, Mr. Rosenberg, who you're citing, is correct, but we are aware of this and we're taking steps as fast as we can in order to increase knowledge and awareness of PIPEDA.

● (1710)

The Chair: Thank you.

You initiated a consultation process, and you've told us about it. I just want to know to what extent you received contributions and feedback in that consultation process from private sector organizations, as distinct from government and the usual suspects, if I could put it that way—specifically private sector.

I think somewhere around 70 people or 70 organizations responded to you, something like that. Of those, how many would have been private sector organizations?

Ms. Jennifer Stoddart: We had 63 respond, 42 from a group—it's kind of a big group—of law firms, financial institutions, unions, universities, industry and professional associations. It's not really broken down as to private and public sector, but I think we have a good response, just looking at them. I would say it's 50% or more from the private sector, clearly. I don't know.

Ms. Heather Black: I think it would be higher than that.

Ms. Jennifer Stoddart: Yes, there was quite an interest.

The Chair: Thank you.

I also understand that you were a former privacy commissioner in Quebec. Given that you were, and I think that regime has order-making power, does it not, we were talking about this earlier, and you've asked not to have order-making power. So I'm curious. Given that you were the privacy commissioner in a jurisdiction where you had order-making power, so you've had a taste of it, if I could put it that way, how is it that you've come over to the side that says “No, I don't want that power; I'm happy with what I have”?

Ms. Jennifer Stoddart: Mr. Chairman, if I may clarify, I'm not saying that to have an efficient privacy regime you should never have order-making power. I'm just saying at this point I think that the wisest thing Parliament could do is let the office go on with the powers in its act, because it hasn't finished using those powers, rather than turning everything upside-down by trying to.... You'd have to completely redraw the legislation.

My experience is that tribunals have their own challenges, notably the challenge of managing the delays of parties. If they're not properly resourced, you have to manage the parties, the availability of those who decide, the presentations of the decisions, and so on. Perhaps for people who haven't worked in tribunals, it seems very quick, a case of we'll just make an order. If you can't rule on damages in order to get your order enforced, then usually one of the parties has to go on to the Superior Court of the local jurisdiction. It's not because you have binding order-making power. It may depend on the legislation that it's necessarily enforced, so you have no damages. You may also be in a very long, drawn-out process, because one of the parties may take you to judicial review during the hearing.

Before this is seen as the panacea in all situations, we should look at exactly what happens in those tribunals, what is their assortment of powers, what elements make them efficient or not. Certainly the ability for us to go to the Federal Court I think is a great advantage. The Federal Court is a prestigious court whose orders will be obeyed and that has the means of enforcing its orders, unlike many administrative tribunals, depending on their design.

The Chair: Thank you, Commissioner.

Mr. Peterson, did you have a question?

Hon. Jim Peterson: It's basically the question you just asked, Mr. Chairman.

What is your sense of how the Quebec and the British Columbia commissions are operating? They have order-making power. Do you think they're hampered by having order-making power?

● (1715)

Ms. Jennifer Stoddart: No, I don't think they're hampered. I know when I was in Quebec that Quebec is very proud it had the first private sector legislation.

You have a law that's set up with order-making power in the cases of those two provinces. I think it's working well in those two provinces within that constituency. I think it's one thing to say it's working well there; it's another thing to take a law that hasn't yet been fully applied and to say, well, after five years let's start again. And that is what I am saying.

You must also be mindful, or doubtless you know, Mr. Chairman, that the model of the ombudsman was chosen because that is the model with which the Privacy Commissioner enforces public sector legislation. It is also the model for the Information Commissioner and for the Commissioner of Official Languages. Because it is this unique federal model, that is why it was chosen for PIPEDA. It was the available model. To change it at this point I think would be very detrimental to the enforcement of private sector privacy in Canada.

Hon. Jim Peterson: Have you ever had a case in which you just couldn't get the results you wanted in a timely manner, and therefore you would have wanted to have that order-making power?

Ms. Jennifer Stoddart: Not for the last year and a half, roughly, when I decided that from now on people complied with our opinions or we met in court—no, with the one exception of the case that's now before the court. There are things like the Blood Tribe case, where we say we don't agree, and we go to court, fine. We each have got a level of court to agree with us, and it's on. But no, not since I've started doing that. I think the issue is how fast we can push through the investigations.

Most of our cases are settled, Mr. Chairman. If you look at our statistics, they're mostly settled. Those that aren't, we'll sit down to discuss it, but if we think we're right, we're prepared to back our word. We haven't had many challenges.

Hon. Jim Peterson: Thank you.

The Chair: Mr. Tilson.

Mr. David Tilson: Thank you, Mr. Chairman.

We talked about the order-making powers. Listening to your experience as the Quebec commissioner, are there other areas that you think could be used in the federal legislation that are not currently in the federal legislation?

Ms. Jennifer Stoddart: I haven't really looked. I'd have to go back and—

Mr. David Tilson: Go back in time.

Ms. Jennifer Stoddart: —look and see if there were any aspects. The laws are fairly similar.

The Quebec legislation now is at the disadvantage of being the first legislation that was written. There are things, I think, that are clearer in PIPEDA now, and clearer in the B.C. and Alberta legislation, and the two laws are substantially similar. So I can't really think of any advantage.

Of course, it's a different model. It's a model. It's an administrative tribunal model, so everything.... Once it goes to court, there is a role. Of course all the observers and experts look at the role and see who's on the role, but that comes with the model.

Mr. David Tilson: Thank you.

The Chair: Thank you, Madam Commissioner.

You are in a very unique position, because you have been able to sit in both chairs with different powers. So if something does come to you before your next appearance before us, we'd certainly appreciate it if you quantified it for us and gave us the benefit of that dual experience, which I don't think anyone else has.

Thank you very much for coming today. We certainly appreciate it.

I want to remind committee members that there will be a meeting on Wednesday from 3:30, and the steering committee will meet next week at some point, to discuss the number of witnesses and a work plan with a finite end to it.

Once again, thank you so much for coming today.

The meeting is adjourned.

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
