House of Commons
CANADA

# Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 033 • 1st SESSION • 39th PARLIAMENT

**EVIDENCE**

## Thursday, February 22, 2007

---

## Chair

**Mr. Tom Wappel**

# Standing Committee on Access to Information, Privacy and Ethics

**Thursday, February 22, 2007**

● (0905)

[*English*]

**The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)):** I'd like to call the meeting to order, please.

I wish to apologize to our witnesses and to my colleagues for being late. I was misinformed as to the room number, and then when I called the committee room there was no answer to the telephone, so I apologize.

We welcome today, for meeting number 33, from the Office of the Privacy Commissioner, Jennifer Stoddart, Privacy Commissioner, and Heather Black, assistant commissioner, who were kind enough to give us even more reading material before their appearance. Thank you for that.

We'll start with an opening statement, one presumes, from the commissioner.

Welcome.

**Ms. Jennifer Stoddart (Privacy Commissioner, Office of the Privacy Commissioner of Canada):** Thank you very much, Mr. Chairman and committee members.

You have met Assistant Commissioner Heather Black, who has been here before and will present part of our position this morning.

We previously sent you the reading material that the chairman just referred to. We did this in an attempt to make reference materials organized and easy for you to consult.

I don't have a prepared opening statement. I'll simply remind you of our position, which we have tried to summarize for you in a way that I hope you found useful. It's on the second, unnumbered page, opposite the table of contents.

[*Translation*]

The summary is on the page across from the table of contents.

[*English*]

right at the beginning, on the right-hand side.

[*Translation*]

You can see a summary of our position in both English and French. There, we include suggestions on amendments to the legislation, as well as state the points we believe require no recommendation.

[*English*]

Just to summarize very quickly, you've heard many witnesses, from most walks of life in Canadian society. You've seen a wide variety of opinions. Some of them are radically opposite one from the other.

In our presentation, we're going to try to advise you on the reform of the law in a way that is both privacy-protective and takes into account wherever possible any consensus or any reasonable position that we could move to, given some of the diametrically opposed positions on these issues.

Let me begin, at the bottom of the first group of bullets, with the changes we would recommend you make in your report on possible PIPEDA modification.

Cooperation with other enforcement authorities is extremely important in a globalized world. The drafters of PIPEDA did a good job in ensuring my ability to cooperate fully with the provinces. For greater certainty on this, we would suggest that you extend that.

The duty to notify possible victims about data breach has emerged in the last few months in a very critical way. I am suggesting, honourable members, that your committee suggest there be a compulsory duty to notify about any violations in the security within which personal information is kept on behalf of Canadians.

I have some material on that. You'll see that we did a résumé in appendix 6. There's an overview of existing American data breach laws that can inspire you as to what would be the composite elements of a duty to notify.

Another practical issue that has arisen is the omission from PIPEDA of the disclosure of personal information before the transfer of businesses. This is known colloquially as due diligence. This is simply an omission. We suggest that you move to have this modified.

We have given as an example, in appendix 2 in your binder, the Alberta model, which we think is a reasonable model to follow.

Again, on the same level of omissions from PIPEDA, we think you could widen the public interest exceptions to consent in cases of emergency, such things as accident victims, dental records being required to identify after death, humanitarian grounds, and elder abuse, which was brought up by the banks, and so on.

● (0910)

[*Translation*]

To the notion of attempted collection without consent, we should add the notion of wilfulness. The Federal Court states that if an attempt is made to collect an employee's personal information, but the attempt is not successful, the legislation does not apply. So that notion of wilfulness needs to be included.

Lastly, when it comes to the thorny issue of national security, in section 7(1), our position is and has always been that PIPEDA should keep the form it had before the amendments brought to it in 2004 by the Public Safety Act. PIPEDA should return to its previous provisions, under which companies did not become agents of the state for the purposes of collecting personal information in order to provide it to security authorities.

[*English*]

Heather Black will go on to talk about the other three suggestions we make to you for legal reform.

**Ms. Heather Black (Assistant Commissioner (PIPEDA), Office of the Privacy Commissioner of Canada):** Moving right along to the employer-employee relationship, it has become clear to us over the past six years that the consent model doesn't work very well in that context. We would propose that you consider the wording from the Alberta law, which establishes a reasonableness test, and temper it with the added notion of dignity of the person, from the Quebec law.

While we say that the consent model doesn't work very well, we are still concerned about the imbalance of power between employers and employees. We always need to consider that things employers are trying to do may not always sit very well with employees.

Business contact information is a relatively simple fix. There's already an exception to personal information. We would suggest it be broadened somewhat to include all business contact information, but that the exception be limited to the purposes of contacting an individual in their business capacity.

Solicitor-client privilege for us is a huge issue, as a result of decisions by the Federal Court. Individuals under PIPEDA have a right of access to their personal information. There are exceptions to that right of access. One of those exceptions is that the information is privileged.

We are not suggesting that privileged information be turned over to individuals. What we would like to be able to do is see that information, to ensure that the privilege is correctly being invoked. That's a very narrow focus, and it's all we're really asking for.

**Ms. Jennifer Stoddart:** Thank you.

I would then like to move down to the areas where we're not recommending any changes and briefly explain to you why.

On the issue of the commissioner's powers, I maintain my position that this is not the time, given all the upheaval in the Office of the Privacy Commissioner and given the fact that we are one of the agents of Parliament and closely linked to other agents of Parliament legislatively, to do a wholesale change in the office.

The act, as it is presently constituted, has a number of powers. We've not had time to use all of them, so I would recommend the status quo on that.

You heard that the process of designating investigative bodies is seen by many as long and cumbersome. I'm not in a position to deny that it is. But I think the opposite—having no regulation and no approval process for investigative bodies—means that we have an open season for self-appointed detective agencies, spy agencies, and so on. It's a very good thing that the federal government has some process for regulating these: they would be operating until somebody made a complaint or somehow they came to our attention, which is very difficult in a country as large as Canada.

Blanket consent has not really been an issue at all, so we suggest we simply pass on that one.

Heather, could you talk about work product and our position on that?

● (0915)

**Ms. Heather Black:** You've heard a lot about work product. Our experience indicates that in many cases work product is not essentially personal information. There are some circumstances where something that appears on the face of it to be work product could be personal information, in that it reveals something about the individual.

We are recommending that we continue to operate the way we have in the past, which is to say that we look at these things on a case-by-case basis.

You may have more questions about work product, but that's essentially our position now.

**Ms. Jennifer Stoddart:** Thank you.

Just to conclude, the issue of transborder flows of personal information is an issue that in our opinion we can deal with through the law as it stands and through contractual provisions in the private sector. I refer you to my first request, that we reinforce our ability to cooperate with other entities throughout the world.

Finally, I'd conclude with something that is not in PIPEDA but I think is a huge problem, and I took the liberty of addressing to this committee, Mr. Chairman, a copy of the letter I sent to Mr. Bernier on the issue of spam. I believe this has been distributed to you. I'm taking this opportunity, as you are the committee that deals with privacy matters, to remind you of how serious this problem is, how privacy-invasive it is.

[*Translation*]

The fact that we are the only G8 country not to have any legislation against spam is very worrying. I would encourage you to focus on the issue.

Mr. Chairman, that concludes our remarks. We would be pleased to answer any questions by committee members.

[*English*]

**The Chair:** Thank you very much.

I'm sure there will be a few.

We'll start with Mr. Peterson for seven minutes.

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

We received a very detailed submission from IMS on the work product issue, with precise wording as to what we should put into it. Could you just tell me why you disagree with what they're suggesting?

**Ms. Jennifer Stoddart:** The law, as it is and as it has been interpreted, already distinguishes work product on the basis that it isn't personal information. So we are concerned that there's no reason to carve out for any particular constituency any type of personal information at this time.

Secondly, we're concerned, as you will see in the appendix that we submitted to this committee, that any kind of carve-out has an indirect effect on surveillance issues.

We're also concerned that if the members think of legislating in terms of work product, they take into account the context in which this particular amendment is requested, the particular industry that this request is involved in, and the legislative initiatives in other provinces that call, for example, in one province, for the consent of those whose work product it is.

That I think is a résumé of why we think it's inappropriate to proceed at this time with that.

**Hon. Jim Peterson:** What is this provincial legislation you're talking about?

**Ms. Jennifer Stoddart:** I'm referring specifically to the Quebec modification of its law in order to accurately capture work product—and this is summarized, honourable member, very briefly in 11 and in our appendix—in Quebec. And because, quite frankly, we're only talking in this case about prescribing habits, those whose prescribing habits would be captured are given, number one, the opportunity to be consulted, and secondly, the opportunity to opt out, neither of which are in this recommendation. I also point to the other provinces' particular experience, for instance, B.C. where there is a ban on collecting this type of information—

● (0920)

**Hon. Jim Peterson:** But that comes through other legislation, doesn't it, as opposed to their access and privacy laws?

**Ms. Jennifer Stoddart:** It does.

**Hon. Jim Peterson:** Our role is to deal with access and privacy. If there are other laws in place that say we don't want this information going to drug salespersons, that's not our business, is it?

**Ms. Jennifer Stoddart:** I think it is, honourable member, because you don't have a wide, shall we say, request for this kind of amendment. It doesn't seem to touch a huge variety of sectors. It seems to be focused. So I submit to you that, given that focus, you have to look at the context and the different laws that apply to have a result in various jurisdictions.

**Hon. Jim Peterson:** I don't think we should deal with the distribution of medical information through the privacy laws. Isn't that the responsibility of provinces and not of the federal government?

**Ms. Jennifer Stoddart:** Well, part of PIPEDA regulates de facto the personal information in the hands of doctors. Because part of medical information is in fact commercial information, and increasingly so, PIPEDA does have that effect and has since its inception, as I understand it.

**Hon. Jim Peterson:** I'm not sure I can agree with you, Commissioner.

Let me go on to your duty to notify. You are now proposing to us a compulsory duty to notify of all breaches?

**Ms. Jennifer Stoddart:** Of all significant breaches.

**Hon. Jim Peterson:** And how do we define “significant”?

**Ms. Jennifer Stoddart:** That's something that we tried to provide as much material as possible for you. We did the survey of the American experience, so it's there for you and for eventual drafters of, we hope, this change.

Clearly, we don't want the public alarmed with something that is not significant, something that is lost and found from one person maybe the next day. There has to be, I think, some threshold that it is significant, highly likely to cause harm.

**Hon. Jim Peterson:** You're aware of the fact that a number of groups, particularly one that the Canadian Chamber of Commerce is involved in, are looking at guidelines that would assist us in this area? Are you working with them on these guidelines?

**Ms. Jennifer Stoddart:** Yes, my office is working with them on these guidelines. I've spoken to representatives of the private sector, and I believe we're meeting with them in the month of March.

**Hon. Jim Peterson:** If your amendment went through, these guidelines would be attempting to define what “significant” means?

**Ms. Jennifer Stoddart:** First of all, it would depend on the sequencing of a possible amendment and guidelines. Clearly, we'll work to guidelines as soon as possible, because I think businesses are interested in guidelines. The Canadian public would feel more reassured by guidelines.

If the legislation were to pass rapidly, then I think eventual guidelines would become much more functional and have an interpretive value, depending on what would be adopted as legislation.

**Hon. Jim Peterson:** In effect, your making reporting of significant breaches compulsory is not going to change practice. You are going to look at these on a case-by-case basis. You will be working on an ongoing basis with the institution and you will be working with the private sector to figure out guidelines as to when it will actually be necessary to report a breach.

**Ms. Jennifer Stoddart:** That's right, honourable member, yes.

**Hon. Jim Peterson:** I understand.

Lastly, I'm worried that we're building up a patchwork of laws across the country—the feds and four provinces now, and how many more provinces to come in the future, I don't know.

Do you ever envisage the situation in which we will have a totally harmonized law in order to make compliance easy with all the provinces and the feds?

● (0925)

**Ms. Jennifer Stoddart:** I think as we move forward all the jurisdictions will increasingly work together by choice because of the central importance of personal information flow in what's more and more a service economy.

Also, because we're a fairly cohesive group, we look and see what works well in one jurisdiction and what doesn't work well as regulators. I think privacy advocates do that and certainly business does that. So I see that we'll have a common learning experience and we will move to a harmonious....

Yes, did you want to—

**Hon. Jim Peterson:** It would sure make compliance a lot easier.

**The Chair:** You're over your time.

**Hon. Jim Peterson:** Oh, sorry, excuse me.

**The Chair:** Did you want to add a comment, Madam Black?

**Ms. Heather Black:** I did. When Parliament enacted PIPEDA, they anticipated the possibility that we could wind up with a patchwork, and that's why the provision for "substantially similar" is in there. It's an attempt to guide provinces towards some sort of harmonization.

Although when you look at the B.C. and Alberta laws that were passed subsequent to PIPEDA, and on the face of it they appear different because they're different drafting styles and they didn't go with the code and all of that stuff, nevertheless all of the principles in the CSA code are embodied in those two statutes. So they are in effect the same. They have minor differences but essentially operate the same way. I don't think business has a lot of trouble complying with all three.

**The Chair:** Thank you.

Before we go to Monsieur Vincent, just so I'm clear, and the commissioner is clear, the issue of work product was addressed by IMS and a number of witnesses. In fact a number of witnesses, including the Insurance Bureau of Canada, recommended that we adopt the British Columbia model of work product.

I'm afraid it isn't as limited as you indicated, Commissioner.

**Ms. Jennifer Stoddart:** Mr. Chairman, may I reply? I don't think I said one witness. I think it is centred around particularly one issue, which is prescription habits, and also, in the case of the insurance industry, on issues of access to doctors' opinions of people they evaluate for insurance purposes. So I remain—

**The Chair:** That's at least two issues.

Thank you.

**Ms. Jennifer Stoddart:** Okay.

[*Translation*]

**The Chair:** Good morning, Ms. Lavallée. You have seven minutes.

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

I believe that seven minutes will not be enough for me to ask all the questions I have.

First of all, I would like to thank you both for being here this morning. I think this will be a very significant meeting.

As I said, I have a number of questions and I don't know with which I should start since they all seem very important to me.

First of all, Mr. Peterson talked about harmonizing and combining all the legislation. If I may, Mr. Peterson, I would like to say that I do not really agree with you. In my view, the provinces sometimes go much further than the federal government. Quebec in particular is frequently a leader in many areas, and I cannot envisage a situation where we would have to be subject to the dictates of Ottawa.

Moreover, the issue of work product was mentioned by a number of witnesses. Representatives of IMS Health Canada even suggested a particular wording. What would the repercussions be if we were to pass the wording suggested by IMS? Have you read that wording?

**Ms. Jennifer Stoddart:** Yes.

I would refer you to the brief we submitted. I believe this is a very significant act. First of all, I'd like to point out what we seem to be forgetting—the current interpretation creates an exception, and implies that PIPEDA does not apply to the situations envisaged by IMS.

Thus, in the interpretations, we recognize the issue of work product where information—in Quebec—is considered personal professional information. We believe that it would not be a good idea to amend the act, given that the status quo is already the goal we seek. Amending the act, which took years of discussion to craft, would be very significant indeed.

If you were to amend the act, you should examine all the circumstances in which the amendments would be required. You should also examine all the possible implications of the amendments, particularly worker monitoring and intellectual product monitoring in other fields, and with people other than physicians or health workers.

I would repeat that, in my view, the status quo already establishes that such situations are not covered by PIPEDA.

● (0930)

**Mrs. Carole Lavallée:** So, if I understand you correctly, the IMS definition would have to be submitted to other groups, such as groups that look after artists' copyright, to see whether it would result in any unintended effects.

**Ms. Jennifer Stoddart:** You could do that, that would be one idea. However, you do not need to adopt this amendment, because the way in which the act is interpreted at the moment means that doctors' prescriptions are not covered by the PIPEDA. Consequently, why pass the amendment?

**Mrs. Carole Lavallée:** I see.

**Ms. Jennifer Stoddart:** If problems are identified, they will have to be dealt with. This has not been a problem, because these prescriptions are actually exempt from the act.

We have identified quite enough problems that led us to ask for amendments to the act. There is a case before the courts—I believe there has been a discontinuance—in which the point was made that in this specific case and in light of the facts of the case, these practices were not covered by PIPEDA.

So I fail to see why you would pass an amendment, if this has not been a problem to date.

**Mrs. Carole Lavallée:** It is probably because IMS wants to be doubly sure—to wear both a belt and braces.

**Ms. Jennifer Stoddart:** That may be it.

What concerns me is that there be at least a belt. But in many cases, under the act, Canadians do not even have that much protection.

**Mrs. Carole Lavallée:** Indeed, particularly with respect to the Patriot Act, which you mentioned earlier. It is quite reasonable to fear that the American legislation may have a very significant impact in Canada and Quebec. Earlier you were saying that under the current legislation, you could manage to ensure that the personal information of Quebeckers or Canadians was protected from the Patriot Act.

What did you mean exactly?

**Ms. Jennifer Stoddart:** No law can protect the personal information of a citizen who is outside the country. All countries have the authority to govern what goes on within their own borders. In light of the importance of trade in the Canadian context and the many situations that could arise, the idea is to find a solution that can be adapted to various situations. I think the solution provided for in PIPEDA is that anyone who exports the personal information of Canadians must require that the person to whom the information is sent, even if he or she is in a different country, will comply with Canadian standards. In Canada, that individual is responsible for what happens. This is handy, because if there is a problem with my information in the United States, for example, and if I have these contracts, I have some recourse in Canada, which is more realistic.

I think that when the Quebec law was amended recently, a standard was introduced whereby data are to be exported only if care is taken to ensure that local standards apply to the export of information.

**Mrs. Carole Lavallée:** You have said if a Canadian company located in Canada exports personal information, there is some recourse. Who has this recourse? Were you referring to the commissioner or to the individual citizen in question?

● (0935)

**Ms. Jennifer Stoddart:** No, I was putting myself in the position of a consumer who has recourse in Canada, or in Quebec under the Quebec act for a breach of contract because of what happened to his or her data abroad, if the Canadian or Quebec standards are not complied with.

**Mrs. Carole Lavallée:** But you know that in a case like that, the recourse is somewhat like David versus Goliath. There are some companies that are responsible enough to send consumers a letter saying that they apologize because they forgot to do this, lost something or whatever. But, even with a letter of this type, what do you expect the average person to do? Only a small minority of people could afford to take legal action against a large Canadian company with ties to the United States.

**Ms. Jennifer Stoddart:** People might have some hope in Quebec, where class actions are relatively easy, compared to the other provinces. People can turn to the Small Claims Court. There are a number of remedies in Quebec that may not exist in the other provinces. However, anyone can make a complaint to the Privacy Commissioner, and we can take action on his or her behalf.

If someone were to submit a complaint about this, I would find it most interesting. We have not had any so far, but I would be pleased to go to the courts with evidence of damages or breach of contract.

**Mrs. Carole Lavallée:** Thank you.

**The Chair:** Thank you Madam. The time is up. You are quite right: it is very short.

**Mrs. Carole Lavallée:** I had such a good question to ask, Mr. Chairman; it was the best.

[*English*]

**The Chair:** Mr. Dewar, you have seven minutes; so far, each of the others has had eight, so....

**Mr. Paul Dewar (Ottawa Centre, NDP):** Thank you, Mr. Chair, and thank you to our guests today.

I actually wanted to shine a little light on something that isn't in the brief here, but it has happened most recently. It's a bill that went through Parliament and is on its way to the Senate, and that of course is Bill C-31, which touches on privacy issues.

It's interesting that while we're trying to deal with privacy here, we seem to be opening up opportunities for people who want to exploit privacy in other places in this precinct. That's because in Bill C-31, An Act to amend the Canada Elections Act and the Public Service Employment Act, in the original legislation, they provided birthdate information for purposes of verification of voters. I wrote to you about this concern I had, and that we have in our party, and the fact that it was then amended to further extend that information to political parties. I wrote to you on that; you sent me a letter last week, and I thank you for that.

I just want to clear something up. As recently as Tuesday, in a question in the House, I asked the government if they would be—

**The Chair:** Mr. Dewar, excuse me. I don't want to interrupt your train of thought, but I mentioned at the last meeting—

**Mr. Paul Dewar:** Sure.

**The Chair:** —that this is a review of PIPEDA.

**Mr. Paul Dewar:** Correct. I'll get to that.

**The Chair:** Will you please bring your questions towards PIPEDA?

**Mr. Paul Dewar:** Sure.

The government was saying to me and was saying to Canadians that your statement to the Standing Committee on Procedure and House Affairs last spring, in June, was that you didn't have concerns that the sharing of birthdate information could affect Canadians' privacy. In fact, in the letter you sent to me most recently—because in June there wasn't a bill in front of us, so you didn't have the privilege of seeing that—there are concerns that I have. I just want your take on the whole business of sharing birthdate information among political parties, and, for that matter, sharing it out there in the public sphere with those who work for Elections Canada.

Here we are trying to protect privacy, and it seems that this legislation will make citizens' privacy a little vulnerable. I just wanted your take on your concerns on the sharing of birthdate information.

**The Chair:** Okay, Mr. Dewar. You know, you're a guest, in the sense that you're not a permanent member of the committee. This is a very specific piece of legislation—

**Mr. Paul Dewar:** Exactly.

**The Chair:** —and your attempt to tie into a review of PIPEDA with your question is admirable, but I can't see the relevance of the question of birthdate information in the review of this particular act.

**Mr. Paul Dewar:** Well, duty to notify comes to mind. For instance, the birthdate information comes from—I'm not sure if you're aware, but Canadians are becoming aware that their income tax form is now shared with Elections Canada through this legislation. I'm just looking at the duty to notify. Has this been considered? This is new and is coming in front of the Senate, and if it's passed, it will affect duty to notify. That's just one.

I could go through a number of other tangential points to PIPEDA, because this is new and I think it's relevant. If we're spiriting this through, people quite rightly want to get on this issue. I think it's important that it be put in front, so that a year from now we don't end up asking why this committee didn't consider this new development.

**The Chair:** I'm going to let the commissioner address whether—

**Mr. Paul Dewar:** That's all I'm asking, and then—

● (0940)

**The Chair:** —she considers it relevant to this issue, and if she wants to—

**Mr. Paul Dewar:** —I'll get right back to the....

**The Chair:** Please do, because other committees have had an opportunity to examine that bill.

**Mr. Paul Dewar:** It was one, and it was not with her.

**The Chair:** It was also in the Senate.

**Mr. Paul Dewar:** It was not with her.

**Ms. Jennifer Stoddart:** Thank you, Mr. Chairman.

Of course anything dealing with personal information, its circulation, and the permission for it to circulate according to the laws of Canada is an important part of privacy. I refer the honourable member, Mr. Dewar, to the letter I wrote him trying to explain this.

To clarify my position, I'll say that in general we have to consider that the birthdate of somebody is key identifying information. In our society it is used in a way that unlocks the door to a lot of important personal information, so it should only be used very sparingly and when absolutely necessary. That's my position, and that's the philosophy that inspires my position on PIPEDA and any other advice that I would give the committee.

**The Chair:** Can we get to PIPEDA, then, Mr. Dewar?

**Mr. Paul Dewar:** I think we did, and thank you to our witness for doing that.

I just want to get back to the duty to notify. In terms of your point 12, you talk about duty to notify and say, "We strongly encourage the Committee to recommend amending the Act to include a breach notification provision." Our party supports that very strongly. We know that this provision and what you're recommending here exist in 32 states. We know that approximately three million Canadians have had their credit cards compromised—I'll use that word—with no financial loss in some cases, but with no notification. I'm hearing from constituents, and I hear generally from my colleague Mr. Martin, who's been following this, that it's a real issue when people find out something happened and they weren't aware of it because of the failure to notify.

Could you expand a little bit on why this is important, and why you say you're strongly encouraged? I would say we should have it, but just give us a little bit more on the importance of having this provision and this change.

**Ms. Jennifer Stoddart:** The events of the last few months, which I think most of the honourable members would have followed, suggest very strongly that this would be an important addition to the law, so that there is no hesitation on the part of companies and organizations holding personal information on behalf of Canadians that when this happens, they do have to take positive steps to notify them and to make them aware and to take action to prevent identity theft.

There was a reputable study done in the United States about the link between data breach and identity theft, because that's always the question: how do we know that data breaches are linked eventually to some harm, because many of them aren't? The study suggested that 5% of those people whose personal information has been obtained because of a data breach would be subject to identity theft. I find that very interesting. If people say that a data breach does not necessarily mean that something is going to happen to you, it would seem from this study that it will happen to 5% of the people. So if you have a breach of the personal information of 100,000 Canadians, then this would suggest that 5,000 of them are going to have serious issues with fraud, identity theft, or the same.

That's a very recent study and that finding is significant. That's why I'm asking this committee to move to make this mandatory, so that we'll have increased attention on the part of organizations to the security in which they keep personal information and then to their duty to act swiftly and appropriately to help people take the right steps to monitor their personal information and their credit cards and even in some cases their mortgages, their land holdings, so that they'll at least be aware. If you don't know that you've been a victim of a data breach, you may not be paying special attention. How many of us have time to read all our credit card statements in detail and so on? I think that's true of many Canadians in their busy lives.

I think this is an important public measure. I have more suggestions for the contents of data breach notification, given our research, and I'd be very happy to help the committee if you were to decide to move in this direction.

● (0945)

**The Chair:** Thank you, Mr. Dewar.

Thank you, Madam Commissioner.

Mr. Wallace.

**Mr. Mike Wallace (Burlington, CPC):** Thank you, Commissioner, for being here today.

I just want to say, on behalf of the whole committee, we appreciate the book you provided us with and the list.

I have a couple of really quick questions first and then I want to focus in on the duty to notify.

Are these things that you've provided us listed by priority?

**Ms. Jennifer Stoddart:** Not necessarily, honourable member. We've tried to put them in an order that is compatible to the order in which we presented them, for easy reading and reference.

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

Have you done a financial analysis of how much this would cost us if you get everything you want?

**Ms. Jennifer Stoddart:** Cost the taxpayers?

**Mr. Mike Wallace:** Yes, because you'd probably ask for more money, would you not?

**Ms. Jennifer Stoddart:** Possibly the only area that would be affected would be the duty to notify because—

**Mr. Mike Wallace:** Okay. Could you provide us with that information, based on any analysis you've done, within the next couple of weeks?

**Ms. Jennifer Stoddart:** We certainly could.

**Mr. Mike Wallace:** Thank you.

Before I make some comments that I want to make to the whole committee in my time, I have a question on the duty to notify. You actually have that power in a sense now with the current legislation. Can you force an organization to publicize?

I got a letter from my company recently that one of my mutual funds got lost or something, and I saw the letter and I threw it out. Where does your power lie now on the duty-to-notify issue?

**Ms. Jennifer Stoddart:** We consider that it's part of the duty to provide security for the safeguard of personal information, and then our powers are the normal powers that we have.

**Mr. Mike Wallace:** Of the recent episodes that we've had in the newspaper, whether it was a local retail facility or a credit card, or in my case with my mutual fund, was your office involved in encouraging those individual organizations to notify their customers?

**Ms. Jennifer Stoddart:** Yes, it was. The organizations got in touch with us, and this has been the practice over the years. Major organizations have a close relationship with the office, and when there is a problem, as far as we know, they usually notify us. We don't know about situations when they don't notify us.

**Mr. Mike Wallace:** So in practice it's been a pretty good process, as far as you know.

**Ms. Jennifer Stoddart:** Yes. What we don't know and what I can't provide you any hard facts on is what we're notified about and what we're not notified about and how quickly we're notified.

**Mr. Mike Wallace:** I'm sorry I'm rushing, but I only have seven minutes and I have lots of questions.

Do you have an opinion on how you define what is notification? Is that a newspaper article or a direct letter to customers? Do you have that?

**Ms. Jennifer Stoddart:** Yes, we do.

**Mr. Mike Wallace:** You've provided an overview on each page, and I've read it. It's very good. I didn't actually agree with everything.

Is there a reason you didn't provide actual wording changes to the act?

**Ms. Jennifer Stoddart:** Yes, because we think that is the job of drafters.

**Mr. Mike Wallace:** Okay, I appreciate that.

What my suggestion to committee will be at the end of this.... We've heard from you right from the beginning, and at first you came and said basically the legislation is working. We heard from a number of private sector groups. It's only been around for the private sector for a couple of years. I personally think we're a little bit premature in reviewing this, so I'll give you a chance to comment on that. The other thing is we've not heard about a lot of changes from you, and then you provided these, some changes, based probably on testimony and issues.

The other piece is I'm interested in giving the minister an opportunity to have a look at what's been before us. So I'm going to be recommending to the committee that we ask the staff, the researchers, to do an interim report that we're able to provide to the minister before he appears before us—it happens to be a he—so that he can respond to issues, similar to what you've basically done here.

One, do you think that's an appropriate approach? And two, the legislation is only two years old and it may take a little longer for us to be able to review it properly. I want to know how you feel about the two-year issue.

● (0950)

**Ms. Jennifer Stoddart:** Would you like quick answers, honourable member?

**Mr. Mike Wallace:** Yes.

**Ms. Jennifer Stoddart:** Mr. Chairman, first, I don't think it's my role to comment on the appropriate way for the committee to work. I think that's really beyond my knowledge as to whether you should make an interim report.

Secondly, I'd remind the honourable member that this legislation was passed in 2000, that banks and other federally regulated organizations have been subject to this legislation since 2001. It came in by phases. The last phase was 2003, so that's four years ago. So it's not that recent.

**Mr. Mike Wallace:** The final phase was 2004, right?

**Ms. Heather Black:** The final phase, yes.

**Mr. Mike Wallace:** So it was just three years ago. All right.

How much time do I have left?

**The Chair:** You have one minute and 40 seconds.

**Mr. Mike Wallace:** Okay, very good.

The question I have is this. We've heard a lot during the presentations about the work product piece. One organization has brought actual wording from other privacy legislation from another province that it would like to see us use. I don't understand yet exactly why, if it's good enough for British Columbia, it is not good enough for our legislation.

**Ms. Jennifer Stoddart:** Mr. Chairman, may I ask Assistant Commissioner Heather Black to explain our position once again?

**Ms. Heather Black:** British Columbia is the only province that has in fact carved work product out of personal information. I don't know why they made that decision, but they did.

Our position is fundamentally that, as guardians of the privacy of Canadians, anything that has a possibility of derogating from the protection of personal information isn't a good way to go. We have been able to deal with the whole issue of work product—the physician's prescribing habits, all of that stuff—working with the tools we have now in terms of the definition of personal information.

**Mr. Mike Wallace:** We had the privacy commissioner from British Columbia here. Have you consulted with him on whether it has been a problem when administering that legislation out there?

**Ms. Heather Black:** I've spoken to him about it informally. It doesn't appear to have been a problem. I don't know how often he's had to rely on it. I can get more information for you if you would like.

**Mr. Mike Wallace:** Thank you.

Those are my questions at this time.

**The Chair:** Thank you.

I'm not sure I understood you correctly, Mr. Wallace, but this is not a voluntary review. This is required by the statute.

**Mr. Mike Wallace:** I understand that.

**The Chair:** Okay.

We can deal with your other suggestion next week when we begin our discussions in camera.

We will now go to Mr. Pearson for five minutes.

**Mr. Glen Pearson (London North Centre, Lib.):** Madam Commissioner and Assistant Commissioner, thank you for coming.

I've been on this committee for five weeks, but I know that you have been here previously and, from reading things from previous meetings, that you have said you recognize a quantitative difference between work product information and privacy—a person's private information.

Is that correct? Do you still hold to that?

**Ms. Jennifer Stoddart:** Yes.

**Mr. Glen Pearson:** Others are zeroing in on the ethical thing about releasing information, but we've had so many groups coming to us and making suggestions about things. Most of them have been big organizations that have the capacity to do things, but a couple of the groups that have come forward have been smaller business associations and so on. They look at this law and understand that this particular act might be helpful, but it's too onerous on them. What they have told us, almost in a pleading way, is that if we run things on a case-by-case basis, they're not really all that capable of handling it; it's difficult for them. They would rather have something that is more permanent, something they could bank on, because they only have a few employees.

I understand that when you consider a case-by-case basis, you have certain capacities, and some of these larger industries do. I am wondering how you feel about the impact on these smaller organizations of the case-by-case thing and how you took it into account. Do you feel that it could be too onerous?

How can they comply? If it is too onerous, they probably won't comply in the way you would like.

● (0955)

**Ms. Jennifer Stoddart:** Thank you. That's a very interesting question.

In the cases we have decided—and I remind you that 75% of our cases are settled in the course of investigation through mediation—we take into account the context in which we're dealing, and I think that's one of the merits of the case-by-case basis. Is it a corner store? Is it a family business?

We had one recently that was a very small, community-regulated radio station, and the assistant commissioner and I had quite an exchange, because I didn't realize it was that one. We were looking at the wording and what had happened there. We specifically took into account that it was basically a volunteer association, although caught in federal legislation; our expectations were tempered by the fact that this was not a major corporation.

This comes up all the time. We try to administer the law in a way that's sensitive to the burdens of business people all across Canada, and I can't say that we have any particular problem with small businesses. They're perhaps not as sophisticated as the larger ones, but when we explain the law to them, they are very happy to comply, in our experience.

**Mr. Glen Pearson:** Thank you.

The second one, Mr. Chair.... I hope it's okay if I ask this, since you brought it up, but you brought up spam. I've been here five weeks and I've had a number of e-mails and presentations from various groups before they have come here. But I've had a lot of e-mails from average citizens in my constituency about spam. They know I'm on this committee, so they want to talk about it.

We'll be going shortly into deliberations on how we're going to look at this as a committee. Can you give us some guidance or guidelines as to the whole spam issue and how you think we should address it? Could you give us some ways forward on it?

**Ms. Jennifer Stoddart:** Mr. Chairman, could I ask Assistant Commissioner Heather Black to respond to this? She worked with the task force on spam and looked into this question quite closely.

**Ms. Heather Black:** In terms of the law you're reviewing right now, we have a mandate to deal with spam. I thank our lucky stars that most of the population hasn't figured that one out, because we could be drowning in spam—not spam, but in complaints. We have had a couple of spam-related complaints.

The recommendations of the task force would have essentially augmented some of our powers to deal with spam. The true spammers are not organizations with whom we can enter into a dialogue in the way we can with the banks or small business or whatever, because they're not interested in complying with laws. So it would be very difficult for us.

We can deal with your average, unsolicited e-mail that you may get from a large corporation with which you may or may not have a relationship, but the true spam issue is something that essentially can't be dealt with under privacy legislation. It is something for the criminal law or for the Competition Bureau when dealing with misleading advertising and all of that stuff, with heavy criminal penalties. I think that's the only way we're ever going to come to grips with spam.

**The Chair:** Thank you, and thank you, Mr. Pearson.

Mr. Van Kesteren is next, followed by Madame Lavallée.

**Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC):** Thank you, Mr. Chair, and thank you for coming again.

What an experience this has been. I don't know how many Canadians realize what the implications are for PIPEDA. You and I talked about that at some length. The more we explore this, especially new members like Mr. Pearson and me, the more we realize the ramifications, and they are huge.

On most of the issues, the questions have been asked. I was wondering about jurisdiction and I was wondering about work product, but the report is excellent. I don't know if I agree with everything; as Mr. Wallace said, the original position was that we did not need to change it, but of course we had some good testimony, and that led us to believe that maybe we should look at some things. I'm still a little concerned about cost; I'm not convinced that this won't increase the cost. We have to look at that, of course.

There were two areas that concern me the most, the first being the work product, and you gave us your position on that. I'm not quite sure I agree with it.

The other is the collection and disclosure for law enforcement. We were visited by the RCMP and the chiefs of police, and they laid out a very good argument for their investigation. They talked about child pornography, how Internet providers or banks weren't compelled, whether or not they were doing an investigation. Will your recommendations, or do your recommendations, cover their concerns specifically?

● (1000)

**Ms. Jennifer Stoddart:** In fact, our recommendations cover the issue of police obtaining information, but our suggestions are, perhaps not unexpectedly, opposite to the direction that the police recommended to you yesterday. We would like to go back to the pre-Public Safety Act version of PIPEDA.

PIPEDA, as it was passed by this Parliament in 2000, did not make into private companies, through extraordinary powers, prolongations of the state's ability to collect personal information without consent for the purposes of law enforcement and national security. This is a major change in a democracy. It's basically giving private organizations powers akin to that of the police. I protested against it when it was passed in 2004; I keep that position.

The police are concerned whenever they can't get information, and they are concerned that PIPEDA has raised privacy consciousness in many Canadian organizations. These organizations ask, under section 7, if they should be doing this—if they should be handing over this employee information if the police come knocking. This article says they may or they may not, so they are considering it. We think this is quite far enough for law enforcement purposes, and it's discretionary.

As Privacy Commissioner, I have to remind this committee that personal information is part of a person's basic rights as a citizen, as a person. The police should be required to go before the courts if they have serious doubts and serious suspicions and need to get people's sensitive information. Surely our Canadian courts can look at what the police record is—they should not go on fishing expeditions through people's places of work, for example.

**Mr. Dave Van Kesteren:** Do I have a little more time, Mr. Chair?

**The Chair:** You have one minute.

**Mr. Dave Van Kesteren:** Like Mr. Pearson, I have smaller businesses as one of my biggest concerns. It became evident very quickly that PIPEDA seemed to be more of an issue with larger corporations than with smaller corporations. In terms of cost, can your office give us some detailed information? We're looking at the small multinationals versus the small businesses. Are we going to have an enforcement problem? I really see that as a looming area of concern—that we are putting big business requirements on small businesses.

On your end of the stick, are we going to have an enforcement problem? Can we have some type of cost analysis breakdown as to what it is going to cost to enforce?

**Ms. Jennifer Stoddart:** Do you mean in terms of data breach notification?

**Mr. Dave Van Kesteren:** In all these recommendations.

**Ms. Jennifer Stoddart:** I think the cost to our office is minimal, but we could certainly cost out if, as we suggest, corporations had to notify us. Certainly, we have to have some type of notification reception mechanism, and that could be an additional cost, but I'd think it would be minimal in the budget of the Privacy Commissioner.

To come back to your—I'd say appropriate—concern with the cost for small businesses, we have been working with the Canadian Federation of Independent Business. We are rolling out special modules for small businesses. We are testing these modules with members of small business because we are very conscious of not trying to impose additional regulatory burdens on small organizations.

In our experience too, the challenge in applying this law is not with small businesses, because they are anchored in the community. As we become more privacy conscious, if your local business messes up with your personal information, I think there will be community pressure. They'll do it once and they'll learn spontaneously. Each community business doesn't have the amount of personal information that huge multinationals do.

My concern as Privacy Commissioner is not the possible danger from small businesses that are doing their best—and we're trying to help them and we're in constant contact with their associations—but the huge amount of data that is pooled in large organizations where one spill can affect possibly millions.

● (1005)

**Mr. Dave Van Kesteren:** Thank you.

**The Chair:** Just to be clear, so we're not talking about apples and oranges and so the committee is clear, your concern on the security issue is paragraph 7(1)(e), which was added by the Public Safety Act. Is that correct?

**Ms. Jennifer Stoddart:** Yes, it is.

**The Chair:** You want the act to go back to the way it was, which, as I understand, included subsection 7(3), including paragraph 7(3)(c.1), which was added by the committee.

It's paragraph 7(3)(c.1) that the RCMP addressed, not paragraph 7(1)(e).

**Ms. Jennifer Stoddart:** That's right.

**The Chair:** Do I take it then that you have no problem with subsection 7(3), and in particular paragraph (c.1), remaining in the act, since you're calling for it to be pre-Public Safety Act?

I guess Mr. Van Kesteren then was really asking about your comments on paragraph 7(3)(c.1) that the RCMP and others commented on, namely the words "may disclose", for example, and the meaning of "lawful authority".

I'm not going to take up other members' time. I just want to be clear on what we're talking about.

**Ms. Heather Black:** Right.

**The Chair:** If you want to address that later to someone else's question, possibly mine, we'll do it.

**Mr. Mike Wallace:** I'll probably ask that question.

**The Chair:** We'll now go to Madame Lavallée.

[*Translation*]

**Mrs. Carole Lavallée:** Thank you.

I will come back to my wonderful question. There are some companies that are responsible enough, including those that deal with mutual funds. For the moment, legislation does not require that businesses notify clients. A friend of mine received this type of letter. I do not know if he has the same mutual funds as Mr. Wallace. In the letter, that I saw with my own eyes, this person was told that they simply wanted to let them know that they had more or less lost their personal information, but that the risk due to the loss was not very high.

Nothing is very clear. We are not aware of the consequences of the loss, nor of the theft of which they were a victim. People are not quite sure what to do either. Mr. Wallace decided to throw his notice into the garbage, but some people filed that information in their heads under worry and anguish.

Do you not believe, Ms. Stoddart, that the legislation should oblige all businesses to notify their clients, according to reasonable conditions? I know you put forward some proposals in your document. Let us presume that the consumer's financial security is at stake, that the risk is serious enough. I know that you have the necessary resources to identify such situations. Do you not believe that first and foremost, there should be a duty to notify the client? In this notice—and it would be a good idea to have that formula drafted by the people in your office—the risk that the consumer in question is facing could be clearly set out, along with the lost or stolen information. I think that the client should know that. It is not enough to tell him that a little problem has cropped up.

There should also be the possibility of some remedy. You mentioned that in Quebec, it is possible to launch a class action. The fact remains that the legislation we are discussing here was designed for the consumer who receives this kind of letter at home. When one considers a class action suit, it is not easy to know where to begin. The business should be responsible for specifying the type of remedy. It should also—and it was one of our witnesses that put forward this suggestion, which I found interesting—compensate in whole or in part the damages that were caused. How could that be done? By taking certain steps itself, for example by sending out the kind of fraud warning to businesses that collect credit information. Indeed, taking those kinds of steps themselves represents a lot of work.

In short, should businesses not have that duty?

● (1010)

**Ms. Jennifer Stoddart:** I more or less agree with what you have just said. That is what the overview of the situation of the jurisdictions who took such steps indicates.

**Mrs. Carole Lavallée:** And they even talk about compensation for the damages caused?

**Ms. Jennifer Stoddart:** Mr. Chairman, we still don't fully understand the link between the loss of personal information and any potential damage this may cause, for example. However, I completely agree with statements made in relation to fixing any such damage.

We also need to work out whether businesses losing such information should be penalized in some other way. For the time being, we're telling you that those unrestricted individuals must be fully apprised of the details, as you suggested.

**Mrs. Carole Lavallée:** That process will be based on the model you're developing, correct?

**Ms. Jennifer Stoddart:** Yes.

**Mrs. Carole Lavallée:** Otherwise, we run the risk of ending up with all manner of weird and wonderful permutations.

**Ms. Jennifer Stoddart:** A specific model is being recommended to businesses. To give you an example, you have to indicate what occurred; when the loss took place; the type of personal information involved; a fairly precise summary indicating the risk of fraud; advice to individuals as to how to better protect themselves; steps the company needs to take; people who can provide any further assistance; the challenges associated with getting this information out to people, by mail, for instance, given the problem of junk mail with e-mailing, for example.

**Mrs. Carole Lavallée:** So you have a solid response to this issue.

**Ms. Jennifer Stoddart:** Indeed we do, we're talking about the fundamentals when it comes to giving advice.

**The Chair:** Thank you, Ms. Lavallée.

**Mrs. Carole Lavallée:** Already?

[*English*]

**The Chair:** *Oui.*

Mr. Stanton is next, followed by Mr. Martin.

**Mr. Bruce Stanton (Simcoe North, CPC):** Thank you, Mr. Chairman, and welcome, Commissioner and Assistant Commissioner.

First I'd like to apologize to my colleague Mr. Martin. At our last meeting we were discussing, and I'm going to be talking about, subsections 7(3) and 7(1). The copy of the act I have didn't have paragraph 7(1)(e) in it and the connection with collection of information, going back and referring to paragraph 7(3)(c.1) in this case. I see the connection there now, and much of our discussion was based on it, so I apologize to you, sir.

In regard to this question, though, we spent a considerable amount of time, particularly with the witnesses we heard from the law enforcement community, dealing with this issue in subsection 7(3) with respect to the discretion that is provided to the organization in choosing to release the information or not release it.

The law enforcement community suggested that the discretion that's provided in the fact that it says “an organization may disclose” was particularly problematic. I understand the point that protecting personal information is vital under our civil rights, under the independence of the laws that provide individuals.... There's another factor, though, at play here in relation to safety, which we need to find the right balance on.

We heard some very compelling evidence that suggested that in certain circumstances—for example, involving a real-time Internet service provider and a predator online with a young person, where there isn't the time and where law enforcement needs to intervene to stop fraud, to stop a situation in which the public is going to be harmed—they need the ability to have that information.

We spent a considerable amount of time on this question of “may”. Would it be possible to provide in subsection 7(3), for the purposes of an impending urgency or a vital public safety issue, for the organization to be obliged, and not just have the discretion, to provide this information, so that in fact they would be required to provide this personal information in the context of subsection 7(3)?

● (1015)

**Mr. Mike Wallace:** “Authorized” in subsection 7(3).

**Mr. Bruce Stanton:** Authorized? Is that what...?

And they even suggest, yes, to have the law read that the companies are in fact authorized to provide it and are obliged to provide it in these circumstances.

**Ms. Jennifer Stoddart:** Certainly anything is possible. That would be possible, but I wouldn't recommend it as Privacy Commissioner.

Let me suggest that Assistant Commissioner Heather Black talk to you a bit more, because she's worked directly on this.

**Mr. Bruce Stanton:** Yes, please.

**Ms. Heather Black:** In my previous life I was with the Department of Justice and was implicated, if you will, in the drafting of this bill. I've heard all of the arguments from all of the stakeholders and I've heard from the RCMP, and you should know that the industry committee amended the original bill to add paragraph 7(3)(c.1) at the insistence, if you will, of the law enforcement community.

I'm not sure that adding the word “authorized” is going to change anything. The “may” in question is a permissive “may”. “Authorize” means you are authorized to do it. It comes to the same thing. It's semantics; basically you're saying the same thing: you may or you may not. It is up to the organization in question to make that call, as to whether in their view the circumstances warrant disclosing information about individuals to law enforcement without a warrant.

**Mr. Bruce Stanton:** On that particular point, because it's a very vital point, do you think it's right in this case—and perhaps this is starting to get beyond the bounds of our discussions here—that we're leaving the discretion, with that kind of decision, in the hands of an organization that, to be honest, may have some interest in not disclosing it?

We heard, for example, that 30% to 40% of these Internet service providers are very uncooperative with law enforcement about disclosing information, for example, about their customers in the case where you have a crime being committed. In fact, they're not interested in having any cooperation in terms of public safety.

We're getting into a balance here of public safety versus disclosure of information.

**Ms. Heather Black:** I have not heard anything from anybody suggesting that ISPs are reluctant to disclose information in these kinds of circumstances.

**The Chair:** We heard that evidence.

**Ms. Heather Black:** On the ISPs in question, there's a handful of them, when you get right down to it, that provide these services across the country. They are large corporations; they are reputable corporate citizens.

It seems to me that it's a bit of a slippery slope on the privacy side if you start suggesting that organizations should give up personal information to law enforcement in some of these circumstances where it would be entirely possible to get a warrant.

Speaking for the Office of the Privacy Commissioner, I would not advocate such a change.

**The Chair:** Thank you.

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

**The Chair:** Thank you.

It's a very interesting discussion. How do you get a warrant when you're looking for an Alzheimer's patient who wandered away from an old folks' home? They're trying to get information about who the person is and where they live, so they can find out where they might be wandering to. I don't see how you'd get a warrant.

Mr. Martin, you have five minutes.

**Mr. Pat Martin (Winnipeg Centre, NDP):** Perhaps the commissioner wants to answer your intervention, Mr. Chairman.

I'm interested to hear what she has to say.

**Ms. Jennifer Stoddart:** I would like to intervene in your last example, Mr. Chairman.

We suggest that for issues of public safety, humanitarian reasons, and so on, personal information should be shared without consent.

That is far different from the law enforcement public security issue. In our systems, we have judges who are always on call, and certainly large corporations have lawyers to advise them.

I wanted to reassure you on that point.

● (1020)

**The Chair:** Thank you very much.

Mr. Martin.

**Mr. Pat Martin:** Thank you, Commissioner.

It's a pleasure to see both of you again.

Thank you, Mr. Stanton, for the clarification of our conversation in the last meeting. I'm partly to blame because I was unable to cite paragraph 7(1)(e), which I was referring to. I had everything but the number, and then you didn't have it here.

I think we understand each other now. I sense everyone understands the possible problem we were trying to point out. Our source was the information brought to this committee by the commissioner in November 2006, where it was quite clearly cited as a very real problem and concern.

You said you asked for its removal at the time the Public Safety Act was debated. Have you ever publicly called for its removal from PIPEDA, prior to November 2006?

I guess you couldn't have, as there wouldn't have been an opportunity.

**Ms. Jennifer Stoddart:** I believe that in that presentation I made, I continued to mention that we thought it was a disturbing trend that corporations basically had police and national security powers.

**Mr. Pat Martin:** To be deputized, is the language you used.

**Ms. Jennifer Stoddart:** Yes, it's a very disturbing trend from a privacy point of view, and I would refer to that event. It's been a constant position in my office since 2004.

**Mr. Pat Martin:** One of the things you pointed out was that private sector companies aren't bound by the same limits or rules as an agency.

What do you mean by that in terms of a private sector company not having the same limits, regarding reasonable grounds versus suspicion?

**Ms. Jennifer Stoddart:** These are all new areas of law. Basically one of the issues of concern is that people wouldn't have what's called due process.

**Mr. Pat Martin:** Right, with no avenue of recourse.

**Ms. Jennifer Stoddart:** With time, it developed in our legal system that the more power you have, the more due process you have to give somebody. This means that people working for companies can see somebody suspicious, and on their own go and get information on them to pass to the police, without telling the person that they're getting this information, whereas law enforcement couldn't do so.

**Mr. Pat Martin:** This is what worries me. Am I reading correctly that not only could the private organization divulge the information they currently hold, but they could be dispatched to collect brand new information on behalf of the enforcement agency, and then share that with them, again without consent or knowledge?

**Ms. Jennifer Stoddart:** Exactly. They can take the initiative.

**Mr. Pat Martin:** That's scary. That is truly scary.

**Ms. Jennifer Stoddart:** Yes. We have many individual security forces across the country that now have these extraordinary powers.

**Mr. Pat Martin:** Dispatched out there to spy on you. This is getting close to a—

**The Chair:** Mr. Martin, the commissioner said they could take the initiative, not be dispatched by someone else.

**Mr. Pat Martin:** Well, either. They could either act on their own initiative—

**The Chair:** Do you agree with that, that they could be dispatched by the state?

**Mr. Pat Martin:** Asked to by the state.

**Ms. Jennifer Stoddart:** I'd have to reread the act.

**Mr. Pat Martin:** Well, let me read you what I have on this.

**Ms. Jennifer Stoddart:** I would think upon request they would....

**Mr. Pat Martin:** a) an organization can now collect personal information without knowledge or consent for the purpose of making a disclosure to a government agency that has requested the information...and

b) an organization may now collect information on its own initiative to make a subsequent disclosure to a government agency for the aforementioned purposes.

That's the legal interpretation we have of this clause. We should all be concerned.

I think we're muddying the waters, if I may say, by using the example of the pedophile abusing a child in real time and the possibility of terrorist, national security issues. That's what I'm focusing on. I told the RCMP that I could relate to and sympathize with that example—drop all the rules out the window to save that kid. In the case of fishing around a person's private affairs on the suspicion that they may be remotely connected to some possible terrorist initiative, that's what worries me.

**An hon. member:** [*Inaudible—Editor*]

**The Chair:** Let's let Mr. Martin carry on with his questioning. No debate.

● (1025)

**Mr. Pat Martin:** I'm going to run out of time very quickly.

I'd like to make it abundantly clear that, if I'm reading your recommendations correctly, you believe there are 34 states that currently have some duty to notify and you strongly encourage the committee to recommend amending the act to include a breach notification provision. Is that your testimony today?

**Ms. Jennifer Stoddart:** That is correct.

**Mr. Pat Martin:** Isn't that great?

**The Chair:** Time's up.

Mr. Tonks, followed by Mr. Wallace. That's the end of round two.

**Mr. Alan Tonks (York South—Weston, Lib.):** Thank you, Mr. Chairman.

I don't sit on this committee, Ms. Stoddart, so you'll have to allow me some flexibility with respect to my understanding of PIPEDA.

I have gained enough information with respect to the national security issue and the Public Safety Act to leave that to the others to pursue, although I did note that one of the issues you are concerned about was that businesses not be the collectors of information for the state. I understand there's a dilemma in terms of public safety. I'll leave that line of questioning to the committee.

There was one issue that had been brought up that did concern me, and I hope it's not irrelevant to the proceedings. It's on your role with respect to Elections Canada and the issue that was raised with respect to information involving birth certificates, date of birth, and, I suppose, addresses, places of residence. Do you initiate your response on a court order with respect to an investigation that has gone on after an alleged electoral abuse has taken place?

**Ms. Jennifer Stoddart:** Honourable member, we're not involved in the administration of the electoral process. That's exclusively the responsibility of the Chief Electoral Officer.

**Mr. Alan Tonks:** Okay, then, who makes a decision or an adjudication as to whether it goes beyond the provisions in PIPEDA, which are, you said, that right of access? Your role is to determine where privileged information is being abused by Elections Canada, let's say. Who adjudicates on that?

**Ms. Jennifer Stoddart:** The whole administration, the legality of the Elections Act, however it may be modified, is the responsibility of another officer of Parliament, who is the Chief Electoral Officer. It's very hard to see how it would be linked with PIPEDA, which is the private sector legislation.

There's another parallel act, the Privacy Act, which would apply to any public sector privacy issues that might arise. I don't know that my office has ever been involved in any electoral investigations.

**Mr. Alan Tonks:** Fair enough. Thank you.

With respect to what you described under investigative powers, I have a quote that you were concerned with respect to blanket consent and that we don't get into—I'll actually use the quote—“fishing expeditions” and “open season”. Those are fairly rhetorical terms. Are you satisfied, within the mandate of PIPEDA and your role, that there is a balance with respect to the private sector and the checks and balances that protect the individual? In your role you have the authorities to use discretion.

**Ms. Jennifer Stoddart:** As it turns out, this is more, I suppose, of a theoretical than a real question. We raised it in our initial consultation paper, Mr. Chairman, that we distributed this summer. We found that the majority of respondents—we had 62 responses, I believe—were not really interested in this issue or really didn't have much to say about it. I think there hasn't been much testimony about it before this committee. So we're saying at the moment this is not an issue that we would advise this committee to pursue, given the importance of some of the other issues. It's a question we'll continue to ask ourselves on a case-by-case basis: was there a valid consent, given the context in individual cases?

● (1030)

**The Chair:** Thank you, Mr. Tonks.

Mr. Wallace.

**Mr. Mike Wallace:** Thank you, Mr. Chairman. I have a few more quick questions.

On the notification piece that you're asking for, in terms of it being strengthened, I want to be clear that you're still not asking for order-making powers. You still want to be an ombudsman in this sense. But adding that authority to force people to notify, is that not giving you order-making powers? I'd say it's not because it's not a financial penalty. Is that correct?

**Ms. Jennifer Stoddart:** No. Order-making powers means that the conclusion you get to is directly enforceable in law. We do have powers, but we have to go to the Federal Court and prove our case to have these powers.

**Mr. Mike Wallace:** So you're happy with the way it is now. You'd like to continue that process.

**Ms. Jennifer Stoddart:** That's right.

**Mr. Mike Wallace:** You were having a conversation with Madame Lavallée and, if I caught it correctly, you talked about working on the voluntary notification piece.

**Ms. Jennifer Stoddart:** Yes.

**Mr. Mike Wallace:** It's great that you're working with that organization for a voluntary code of conduct. But doesn't that really exist already in your office in a sense? Isn't there a voluntary system by which they call you and you advise them on how to do it? Doesn't it exist?

**Ms. Jennifer Stoddart:** Yes, some of them call us, but we don't know about the ones that don't call us. It's clear to me as Privacy Commissioner that when this happens it's maybe not clear enough to all corporations exactly what they should be doing. I'm in favour of guidance, while waiting for the amendments to be passed, hopefully. I'd be happy to work on guidelines, so it's very clear when this happens they know what they should notify people about, and that's what Madame Lavallée was suggesting. What are the implications? What are the details? What's the template? Who should be notified? Who should people call? What should they do?

**Mr. Mike Wallace:** I completely understand your role. You're here to protect privacy. You're the Privacy Commissioner and with you is your assistant commissioner. Privacy is your issue. From my end of the table, there has to be a balance between security and privacy in today's environment, whether it's a great thing or not. And to be frank with you, and I know Robert agrees with me, "lawful authority" might be a difficult thing for them to explain. The "may" issue and "authorized" to provide it, I think in terms of wording, aren't a huge change but may help police in describing it.

Just give me an example. We've used this terrible example of the ISP user. We were told there are a thousand ISP providers and about 30%...that's 300, not a few. Now there are a few big ones, but they're small and they may be our problem.

Let's use another example, and tell me if I'm wrong, because I just don't know and I'd like to know this before I make any decisions on it. I own a company that produces guns, for example. I have a customer who happens to be buying guns lawfully but selling them to a group that's on our terrorist list. The police want to know whether that person is my customer. Am I entitled, as the owner of that company, to tell them, based on the law? Do they have to explain to me that I may tell them or I may not? Do you think "authorized" to provide it would help that situation or not, or do you think they really need a warrant to find out whether this person is my customer?

**Ms. Jennifer Stoddart:** The paragraph is permissive. So it's their judgment that if this is something direct, they somehow know that this person is on the terrorist watch list and buying guns.

**Mr. Mike Wallace:** I don't know where he's selling the guns, but he's buying a large amount of them. It's legal and he is entitled to do it.

**Ms. Jennifer Stoddart:** It's their choice; that's what we're saying. In 2000, this choice was already put in.

**Mr. Mike Wallace:** If we change it to "authorized to provide", is that damaging?

**Ms. Jennifer Stoddart:** Yes, because any information that the police or national security forces would want would almost have to be provided. We have a court system for this, and if it's that serious, my position is, why don't you go before the courts?

**The Chair:** No, they would either have to have a warrant or lawful authority—not any information that they want.

**Ms. Jennifer Stoddart:** They say they have lawful authority in terms of—

**Mr. Mike Wallace:** I'm convincing Mr. Vincent that he's going to vote for—

[*Translation*]

**Mrs. Carole Lavallée:** Just for your information, Mr. Chairman, I'd like to point out that a gun registry would be a perfect way of achieving this.

**Some hon. members:** Oh, oh!

[*English*]

**Mr. Mike Wallace:** Thank God for translation—

**Some hon. members:** Oh, oh!

**Mr. Mike Wallace:** —because I can't understand a word she said other than that.

[*Translation*]

**Mrs. Carole Lavallée:** That's one, zero!

[*English*]

**The Chair:** Are you done?

● (1035)

**Mr. Mike Wallace:** Yes.

**The Chair:** Okay, we're going to round three, and I'll start the round.

Then we have no one on the Conservative side, so if somebody wants an opportunity...and then we have Monsieur Vincent.

I have three questions.

Number one, did I understand you correctly, Commissioner, in your opening remarks to say that the act hasn't been around long enough for you to have a chance to use all of your powers yet? Did you say that?

**Ms. Jennifer Stoddart:** I did.

**The Chair:** Okay, what powers have you not used?

**Ms. Jennifer Stoddart:** There are many issues that I've not been able to explore before the Federal Court—for example, the issue of damages. Interestingly, with a lot of foresight, the law provides for damages. I have not yet had a case in which there was a provable amount of damages that wasn't settled beforehand, where I could go to court to see how PIPEDA can help remedy Canadians' actual damages for privacy.

I have a power to do audits on private sector corporations, when I have reasonable grounds to believe that there may be a problem. That is being challenged by one organization. The hearing before the court has not yet come up, so I don't know the extent of this power, which I would argue is an important power.

There are many things, including penal clauses in the act that have not been used. They're not necessarily for me, so I'm just saying that in response to the issue about the commissioner not having power, there is quite a bit of power foreseen in the act, and we should look to see how these powers can be applied before moving to another model.

**The Chair:** Thank you.

The second issue is solicitor-client privilege: Blood Tribe.

Your note is good, thank you. Also, thank you very much for your paper and your comments. They are very helpful.

**Ms. Jennifer Stoddart:** Yes, the staff does that.

**The Chair:** Yes, but they have direction.

This is not numbered. I guess this is point number 1 in your thing, and I quote: “This decision leaves a gap in the Commissioner's powers and will potentially allow” a broad claim of solicitor-client privilege over corporate-held documents to inhibit an OPC investigation, “with no possibility of independent verification” of the appropriateness of the solicitor-client claim, “other than through a formal application to court”.

What's wrong with a formal application to court, for a court to decide whether or not solicitor-client privilege has been lawfully claimed? With no disrespect to your office, I would think that a judge has the expertise and legal training to make that determination better than your office does.

My question is what's wrong with that? Is your concern that it would take too long for a decision to be made on this very specific issue? If so, and if that's the only issue, why can't you make an immediate application to the Federal Court to determine whether or not this particular claim for solicitor-client privilege is lawful? That is the only question.

**Ms. Jennifer Stoddart:** This is what we are doing in compliance now with the recent order of the court of appeal. But could I ask the assistant commissioner to answer your question, because she was directly involved in this case?

**Ms. Heather Black:** It would be a cumbersome thing to have to go through. It's also unclear to me how we would get ourselves into Federal Court to do this, since Federal Court is not a court of inherent jurisdiction. Without some sort of statutory amendment, I'm not sure that we could even get ourselves there.

**The Chair:** That's exactly the point. That's why we're reviewing PIPEDA. You could make a recommendation that we put in the statute that if somebody claims solicitor-client privilege, an application should be made to the Federal Court for the Federal Court to determine whether or not that privilege is properly claimed, if you don't think so. That could have been one of your recommendations.

**Ms. Heather Black:** That would have cost implications as well.

**The Chair:** Clearly, as everything does when it goes to the courts.

**Ms. Jennifer Stoddart:** To follow up on Assistant Commissioner Black's remarks, Mr. Chairman, we have that power under the Privacy Act. When the federal government claims solicitor-client privilege, we can review the documents only to see whether the privilege rightly adheres to the documents for which there's a complaint. That was not put into PIPEDA because for some reason it seemed to be an issue that was solved at that point. Nobody thought it was a problem, I understand, from the drafters. We're simply asking you to bring our powers on a level with those we already have on solicitor-client privilege for the public sector.

**The Chair:** I'm going to confess my bias as a barrister and solicitor in that I think one of the most important fundamental freedoms we have is the strength of the solicitor-client privilege in this country on all issues. Quite frankly, I'm surprised that it's in the Privacy Act, and I have no difficulty personally with requiring a court to make a decision as to whether or not the privilege has been properly claimed. I think that's the proper place for that very important fundamental freedom of individual people to be determined, and not—with all due respect and not to you personally—through a commissioner not reportable to the judiciary.

This is my third and last point, and I'll read this directly from our researcher's question because we want to try to get an answer:

> With respect to the issue of breach notification, we have received a white paper put out by the Canadian Internet Public Policy Interest Clinic in January 2007. CIPPIC advocates a law requiring organizations to notify individuals when certain breach criteria are met.

Have you had a chance to review that paper? What are your comments about it?

● (1040)

**Ms. Jennifer Stoddart:** I think in our written material we say that it's an excellent and very thoughtful paper. Yes, clearly, there has to be a threshold. I gave the illustration earlier in my remarks on when things are lost for 24 hours and so on. You don't want companies to be burdened with every misplaced piece of paper or CD in an office. There have to be threshold requirements for it not to be too burdensome and become irrelevant to consumers and the public too.

**The Chair:** Thank you very much.

Monsieur Vincent, and then Mr. Van Kesteren

[*Translation*]

**Mr. Robert Vincent (Shefford, BQ):** Thank you, Mr. Chairman.

To begin with, I'd like to congratulate Mr. Wallace who has admitted today that he understands the commissioner's role.

[*English*]

**Mr. Mike Wallace:** Thank you.

[*Translation*]

**Mr. Robert Vincent:** Ms. Stoddart, I agree entirely with what you said about police officers, doctors and work products, and when you say that nothing should be revealed. However, I have a bit of trouble with you saying that losing just a single's day worth of information isn't that serious. You don't know who has got their hands on the information. The person may very well bring back the information that very same day, but having the information for just half an hour is half an hour too much. You don't know what the person has done with the information. The individual may have sold it, etc.

I hear my colleagues saying there needs to be a greater focus on small businesses. May I point out, however, that when representatives from the Canadian Federation of Independent Business testified before the committee, they said they provided training to small business operators. Members of the Chamber of Commerce also provide training sessions to small businesses on the legislation. So there shouldn't be any preferential treatment, be it for a small business or otherwise.

In my opinion, small businesses are especially important. A small shop or clothing store may, over the course of the year, have who knows how many clients. How many credit cards pass through their doors? It's especially important for these people to be aware of the importance of protecting the private information they are privileged with.

So on that note, I imagine that businesses should, to some extent, be made accountable under the act. If a small business operator thinks that he or she has lost private information then the client or clients should be contacted immediately. That way they can contact their credit card companies, banks, etc. to make sure nobody else uses their personal information, which may lead to legal hassles for them. Businesses should bear some of the responsibility when information is lost.

If somebody's identity has been stolen and this leads to financial losses or a crime being committed, the industry or the business should be held responsible and pay the individual back.

What's your opinion?

**Ms. Jennifer Stoddart:** I agree with both you and Ms. Lavallée entirely. It's indeed extremely important that businesses waste no time advising consumers in a proper manner.

I wasn't insinuating that the loss of one single day's private information was not significant. It's easy to misplace things throughout the course of the day and if you happen to misplace something in your office and are required to notify somebody immediately, I'd be afraid people would become disillusioned and an unbearable burden would be placed on small businesses.

I agree with you entirely on every other point and I would reiterate that we are working with the Canadian Federation of Independent Business in developing a number of training modules. We're currently testing some educational material with small businesses to make sure that they get the assistance they need so they don't break the law.

● (1045)

**Mr. Robert Vincent:** Do you believe that encouraging small and large businesses to compensate those individuals whose personal information they lost is enough to get them to consider that the personal information they have in their possession has to be dealt with as carefully as if it were their own?

**Ms. Jennifer Stoddart:** I think it is a very important incentive. The public is very concerned by all this. Perhaps you watched *La Facture* last week. This is not the first time that the media has dealt with this phenomenon. We all are very concerned. People are feeling a bit paralyzed. It is very important that people have tools and take action to counter this phenomenon. We have to have the authority to act. The message for businesses is clear: under such circumstances, you have to notify people and tell them what you will do. But I think that things are not that clear at present.

**Mr. Robert Vincent:** Should those incentives not be included in the act, that is to clearly state within the act that all lawyer's fees and costs related to the loss of personal information should be paid by the industry? Could we not include something so that everyone understands?

Both small and large businesses do not take the Privacy Act seriously. I have seen insurance companies sharing information about people who had been involved in car accidents. People from one insurance company would call up staff from another to find out whether a certain individual had already had a car accident while covered by that company. They gladly share personal information. I am not sure that they take serious care of the personal information in their possession.

**Ms. Jennifer Stoddart:** PIPEDA, which you are currently reviewing, already contains a compensation provision. I was talking about it with the chair earlier on. It is possible to obtain compensation. We have raised the issue, and up until now, all businesses have settled their problems out of court. The act therefore does cover such incidents.

Now, when there is a breach of contract or loss of personal information, we want consumers whose personal information is being held to be notified. I think that notifying consumers and businesses would help greatly.

**Mr. Robert Vincent:** Could we not have...

**The Chair:** Mr. Vincent, your time is up. Thank you.

Mr. Van Kesteren, you have seven minutes.

[*English*]

**Mr. Dave Van Kesteren:** Madam Commissioner, I want to talk about spam for a minute. In your submission you said that none of the task force recommendations has been implemented. Wouldn't you agree that some have been adopted by businesses? I'm thinking of the "Stop Spam" website, the volunteer organizations for businesses and organizations to protect their personal information. Isn't that working? Can you just briefly comment?

**Ms. Jennifer Stoddart:** Yes, there is a concerted effort on the part of the private sector and the police to deal with spam as a vehicle for fraud. In fact, in a couple of days it's going to be March, Fraud Awareness Month, and we are going to be very active in that along with many law enforcement agencies, important agencies like the Competition Bureau, the chambers of commerce, and so on. We are all doing our best—

**Mr. Dave Van Kesteren:** The government is backing that.

I'm sorry to interrupt.

**Ms. Jennifer Stoddart:** That's not directly the government. There are government agencies involved in that, yes, you are right. There was a fairly important task force—there were many specialists on this task force—that suggested we have some specific anti-spam legislation. Most of the G-8 countries—I give the statistics in my letter—do have such legislation, and specific measures would help us to fight spam. That's what I wrote the minister about as Fraud Awareness Month approaches.

● (1050)

**Mr. Dave Van Kesteren:** You mentioned that this committee ought to focus on spam. We're conducting a review of PIPEDA. In the report on spam, don't we make any recommendations for any specific changes to PIPEDA already?

**Ms. Jennifer Stoddart:** There were some suggestions for minor changes, but we're not suggesting that PIPEDA be amended wholesale to deal with spam. It's not perhaps the most appropriate vehicle, but I am presuming on this committee's mandate for privacy —this is the House of Commons committee on protection of personal information—to draw to your attention an associated problem that didn't exist, and I don't think it existed really, in 2000 when PIPEDA was created. In the lives of many consumers—and I don't know about you, but we receive a lot of spam—this is a huge threat to our personal information, and it carries fraud implications.

**Mr. Dave Van Kesteren:** How has your office stepped up its enforcement since the report? Have you stepped up enforcement against spam?

**Ms. Jennifer Stoddart:** As Assistant Commissioner Black explained, it's not something that with our existing powers we're really set up to deal with because it takes strong penal criminal powers, but we have stepped up our cooperation on Fraud Awareness Month. Six years ago I'm not sure that existed, and each year that goes by we are playing a bigger and bigger role. You will see a press release. I brought this up at the recent federal-provincial privacy and information commissioners meeting in Banff. You will see some concerted action on the issue of fraud awareness on the part of all the commissioners across Canada. Yes, we are stepping up our education efforts tremendously.

**Mr. Dave Van Kesteren:** I don't think it's been addressed yet, but one of the suggestions by some of the groups was that you should have more teeth. How do you feel about that? I know that when you first came here we all felt, and I agreed, that it's in the best interests of banks and insurance companies and the larger corporations to apply these practices, and you felt that exposing them or making the public aware of breaches would be a deterrent. What do you think about some of the suggestions that you should have more teeth and that there should be fines or things like that in your power? How do you feel about that?

**Ms. Jennifer Stoddart:** I respect the opinions of those who suggest that to you. They're looking at other enforcement models that work very well in that context. But I'm saying to you that given the recent history of the Office of the Privacy Commissioner, and given also that we're not a one-off creature, rather we're linked in the interpretation of our act to the Access to Information Commissioner and to the role of other agents of Parliament, if you look at that and you look at the powers I have, particularly under PIPEDA, I have quite a few teeth as it is. There's been a lag in maybe baring those teeth because of those reasons, but the law has quite a few teeth.

Where I need more teeth is in the Privacy Act, but that's not the subject for today. I need a full set of dentures for the Privacy Act.

**The Chair:** Thank you very much.

Mr. Peterson.

**Hon. Jim Peterson:** Thank you.

Ms. Black, in response to Mr. Pearson, you said there were very few ISPs that we had to be concerned about. We heard testimony that there are well over 100 or so. I just want to clarify—

**Ms. Heather Black:** There are a lot of small ISPs, yes, but the majority of Internet services are provided by essentially a handful of companies in this country, a huge proportion.

**Hon. Jim Peterson:** Thank you.

Ms. Stoddart, if we were to choose, as a committee, to adopt the B.C. model for defining work product, would that cause you problems? If so, what would these be?

**Ms. Jennifer Stoddart:** We've addressed this issue that we are hesitant to recommend that you move to that because the interpretation, perhaps not necessarily by us but it's a direction to the courts as well, could spill over into many areas that we can't foresee at the time and could have an impact on the general issue of worker surveillance, which is a huge issue. Between voice prints, GPSs, biometrics to get in the door, surveillance videos at your work and so on, this is a huge issue for all of us. I would be concerned with the additional direction that it would give me in that context.

● (1055)

**Hon. Jim Peterson:** Were we to adopt it, would there be a way to deal with the concerns you just expressed and yet bring a greater amount of certainty to the question of what work product really is?

**Ms. Jennifer Stoddart:** If you chose to suggest that, perhaps I could look at it in that light and make some suggestions at that point.

**Hon. Jim Peterson:** Good. Thank you.

[*Translation*]

**The Chair:** Mr. Vincent, you have time for a short question. We will then move on to Mr. Stanton.

**Mr. Robert Vincent:** I said earlier that businesses should compensate those people. Instead of going to court, would people not be better off going to see you first, so that you could make a decision regarding a business' responsibility and ask that it reimburse the individual? You are on the front line. In the event that there is no agreement between the two parties, they could go before the courts. That way we could do away with at least one step and reduce legal fees. If people went to see you first, you would have to determine whether the business was responsible for the claimant's financial losses.

**Ms. Jennifer Stoddart:** Absolutely. That is totally part of our mandate. For example, Quebeckers can come to us to file a complaint against a federally-regulated company. The service is free, and we could take care of the damage claim form.

**Mr. Robert Vincent:** Within a reasonable timeframe?

**Ms. Jennifer Stoddart:** Yes.

**Mr. Robert Vincent:** Very well. Thank you.

[*English*]

**The Chair:** You have one short question, Mr. Stanton.

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

I have just one very quick question. In your remarks you mentioned that when there's a breach of privacy, personal information, 5% of that ends up in some type of fraud or criminality. Where does that number come from? Where would you glean that?

**Ms. Jennifer Stoddart:** That comes from a study in the United States. I don't have the exact reference here, but we subscribe to many newsletters that cover the situation. This was a study coming out of the United States that was reproduced in one of these privacy law newsletters.

**The Chair:** Thank you, Mr. Stanton.

Would you be kind enough to provide us with that reference material so that we could have a look at it?

**Ms. Jennifer Stoddart:** Yes, certainly.

**The Chair:** Thank you very much, Commissioner and Assistant Commissioner, for appearing before us. Your paper was very helpful. As you can see, we're struggling with a lot of these issues, and we do appreciate your giving us your views and your guidance at the end as well as you did at the beginning. It was very helpful.

Committee members, I have just two things. Tomorrow you should receive a summary of recommendations by all of the witnesses. That should be in your offices tomorrow, so for those of you who have nothing better to do on the weekend, you have the weekend to review it.

**Mr. Bruce Stanton:** There's nothing I would like better.

**The Chair:** We'll have our first in camera meeting on Tuesday at 9 o'clock. I will find the right room in the right time. Right now it's 237-C, and hopefully we'll see you then to discuss that.

You will recall that at the request of the committee I wrote to the minister asking that he appear. The minister seems to be very busy. I offered many different compromises, including holding a special meeting and having a meeting in the evening, and it would appear that the minister is busy for 24 hours a day until the break. He has finally agreed to appear on March 20. I've indicated to him that the committee will not accept any changes to that, so that's when he will appear.

By that time we will have focused on some of the things we're thinking about that we're either unanimous on or have a majority on, and we can discuss them with him.

Thank you very much. We'll see you next week.

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**

---