House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 028 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Tuesday, February 6, 2007

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 6, 2007

● (0905)

[*English*]

Mr. Mark Yakabuski (Vice-President, Federal Affairs and Ontario, Insurance Bureau of Canada): Mr. Chairman, my name is Mark Yakabuski. I'm going to lead off, if you don't mind, on behalf of the Insurance Bureau of Canada.

The Vice-Chair (Mr. David Tilson): Could you introduce your colleagues?

[*Translation*]

Mr. Mark Yakabuski: Thank you, Mr. Chairman.

I am Mark Yakabuski and I am Vice-President, Federal Affairs and Ontario, with the Insurance Bureau of Canada. I'm joined by Randy Bundus who is IBC's Vice-President, General Counsel and Secretary.

IBC is pleased to be here today to participate in your review of the Personal Information Protection and Electronic Documents Act or PIPEDA. IBC is the national trade association representing the private general insurance companies that provide insurance for homes, cars and businesses.

IBC has been actively involved in the development of private sector privacy laws since the early 1990s. IBC and its members are strong supporters of PIPEDA and the general privacy laws in Alberta, British Columbia and Quebec.

This morning we would like to highlight three issues from our written submission to the committee.

[*English*]

We have three points. We know your time is valuable. The first issue is with respect to work product information. Now I know that you've already had representations on this issue before the committee. There are really two different components to our position with respect to work product information, which we believe can be dealt with by one unique recommendation.

PIPEDA sets out the rules regarding the collection, use, and disclosure of an individual's personal information, as you know, which is identified as identifiable information with respect to an individual. However, PIPEDA does not specifically address the matter of work product information currently, that is, information that is created by a company and its employees in the course of their business activities. This information is not personal information and therefore not regulated by PIPEDA. Yet it is important in our view that PIPEDA be amended to formally recognize work product information, and I'll tell you why.

In a competitive economy—and I know that Parliament wants a competitive economy—it is absolutely essential that companies have access to information about the products and services that they in turn buy from other businesses, so that they can use this information to innovate and improve the products and service they sell their customers.

Without access to work product information, innovation and competition will be stifled in the economy. For insurance companies, for example, we need access to work product information, generated by the many businesses from whom we buy products and services. For example, we need to be able to analyze the quality, the durability, and the effectiveness of the billions of dollars of car repairs that we pay for each year, so that we can improve the service that is offered to our customers. If PIPEDA is not amended to recognize work product information, we believe very strongly that Canadians will be the losers.

Now the second component of work product information can be illustrated by the information in an insurance claims file. A claims file contains both personal information—identifiable information about the claimant—and work product information about the handling of a claim. An individual absolutely ought to have a right to their personal information in the file, but that should not be the case for the work product information that is generated by the company itself. This work product information is created by the insurance company for the purpose of handling that claim and it is important that it be recognized that it is not personal information.

The issue of work product information is too important to be left to an interpretation of PIPEDA and must be addressed and defined in law, in our opinion. We recommend the approach that British Columbia has taken in its Personal Information Protection Act, in which work product information is defined and explicitly recognized as not being personal information.

Mr. Bundus will now speak about two other issues.

Mr. Randy Bundus (Vice-President, General Counsel and Corporate Secretary, Insurance Bureau of Canada): Our second issue is whether an individual can make a request under PIPEDA for access to their personal information at the same time they are suing the insurance company in court. This issue may be unique to property and casualty insurers, which deal not only with their own customers but also with non-customers. We refer to these as third parties. The third parties will say that they have suffered damages or injuries because of the acts of the insurer's customer. The relationship that exists between the third party and the insurer is often adversarial.

The experience of our members is that these access requests are not being made for the PIPEDA-stated purpose of correcting inaccuracies in the information, but rather so that the individual can use information in the insurance claims file to assist them in their court action against the insurer. This should not be allowed to continue. It is prejudicing the ability of insurers to fulfill their legal obligation to defend their customers in any lawsuit.

We recommend that PIPEDA be revised so that the rules of civil procedure that regulate access to information during lawsuits take precedence over PIPEDA when a legal action has been started.

Our third issue also reflects the unique nature of the P and C insurance business in which insurers have to investigate the events of an accident. This includes collecting statements from people who witnessed the accident or who have information about the accident. A witness statement will typically contain information about the witness, the witness's observations of the incident, and information about another individual who was involved in the incident. This other individual is the subject of the statement. A witness statement may as easily confirm and verify the claimant's version of the events as it might cast doubts about the incident. It is to everyone's benefit if all of the relevant facts and information are gathered by the insurer as quickly and accurately as possible.

Witness statements are not specifically addressed in PIPEDA, and this results in uncertainty about their treatment under that law. The first issue is whose personal information a witness statement contains. In our view, the observations of the witness are the witness's personal information, and therefore the witness may freely give a statement to the insurer.

It has been suggested that an insurer should, before collecting a witness statement, obtain the consent of the person who is the subject of the statement. This suggestion defies common sense. It would effectively allow the subject of the witness statement to prevent the witness from reporting what they saw or heard.

We recommend that PIPEDA be revised to clarify that the personal information expressed by a witness is the witness's personal information. PIPEDA should also provide that an organization may, during the course of investigating and settling contractual issues or claims for loss or damages, collect, use and disclose a witness statement without the subject's knowledge or consent.

This morning we have briefly summarized three of our issues and proposed solutions. We would be pleased to answer any questions that you may have on these or any of the other issues in our written submission.

Thank you.

● (0910)

The Vice-Chair (Mr. David Tilson): Thank you very much, gentlemen.

Go ahead, please, Mr. Long.

Mr. Murray Long (President, Murray Long & Associates): Thank you very much for inviting me here today.

I am a self-employed privacy consultant who has been living and breathing PIPEDA since the law was first tabled in Parliament back in 1998. I'm something of a privacy law expert, or at least people refer to me that way. Although I am not a lawyer—and my clients always tell me they're glad I'm not—I'm willing to attempt to answer any questions you may have about the law and give you the best insights I can.

I look forward to a dialogue with you and to the opportunity to address, to the best of my ability, any aspect of the law that you wish to ask about and how it works in practice.

PIPEDA is important legislation. It establishes a fundamental right to privacy in the commercial marketplace and sets out a framework under which the interests of citizens in controlling their personal information are balanced against the needs of businesses to collect, use, and disclose it for reasonable purposes.

By and large, this balancing of interests works very well, and by and large, PIPEDA is a good law. In fact, as someone who helped write the CSA code that is a fundamental underpinning of this law, I have found it remarkable at times just to look back on it and notice how durable this law really is. The CSA principles were very well crafted and have stood up very well over the years, despite the fact that there's some complexity in the wording in places.

Despite the lack of clarity, the law is founded upon broad concepts that are solid and provide a basis for reasonable people to make reasonable judgments about how their personal information should be protected. This review process is nevertheless a very important opportunity to fix some problems with the law and to make it even more effective, more efficient for business in some ways, and more fair to the public in others.

To the comments that have been made that it is too soon to hold this review, I would say that is not the case. There are problems that need fixing right now on the basis of six years of application of the act, the insights gained from the next generation laws in Alberta and B.C., and growing concerns over such public issues as identity theft. The work you are doing right now about such problems is extremely important and will have a major impact on making PIPEDA an even better law in the years to come.

From the back rows, I've been intently watching the other witnesses over the past several weeks, and I've decided at this juncture to restrict my formal comments to addressing seven issues. I understand that my brief has not been translated but will be available soon.

I think the seven issues I'll be focusing on in my written submission are all important issues, some of which have not yet received a lot of attention. I'd be pleased to talk about any one of these. They are the question of commissioner powers; access barriers to the Federal Court; consent in the employment relationship; breach disclosure; attempted collection without consent; collection for national security purposes; and collection without knowledge or consent for administrative law purposes.

Of these seven issues, in my oral comments I want to speak about three of them. The first is breach notification.

Identity theft is a major problem and it affects the entire marketplace, even responsible companies that have strong data safeguards and have never encountered a breach. The costs of security breaches and identity theft are borne throughout the marketplace and result in higher costs to goods and services, and as importantly, lead to a diminished public trust in data sharing.

Responsible companies may believe that breach notification rules should be left up to them, and I have no doubt that responsible companies will act responsibly in this regard, mindful of the reputational risk, fiduciary responsibilities, and other such factors. However, as Canadian Marketing Association President John Gustavson once remarked about the need for a privacy law, when he advocated for one, in the world of privacy, the world is not made up of responsible companies.

There needs to be a mechanism that will enforce responsible behaviour throughout the marketplace, especially in this area.

Looking at the mechanics of breach notification, I am proposing a four-point model that I think is clear, fair, strong, realistic, and protects the public interest.

The first point is that there would be a duty to notify that would apply to all types of sensitive information, not just financial data. For example, a breach of health records can cause as much harm and damage to the individual as loss of information that could lead to identity theft.

● (0915)

Secondly, organizations should have some discretion to determine when to notify the public, but that should be based upon not just their own self-assessment on their own factors, but also upon an objective standard such as the reasonable persons standard that is currently embedded in the act, which forces organizations to act prudently.

They must notify the Privacy Commissioner when a reasonable person would consider it appropriate to do so and must make this notification in a short, legally prescribed timeframe following a breach. When they notify the Privacy Commissioner, under my model, they would be required to describe the impacts of the breach, the efforts taken to mitigate it, and what decision was made to notify affected persons. If they decide not to notify persons, which should not happen in most cases, but there could be exceptional circumstances, they must explain why they choose not to. The Privacy Commissioner could then question these decisions that were made.

The really important point about breach exposure, though, is that we need to have enforcement tools, and in this regard I believe it should be an offence under the act to fail to disclose notice of a breach where a reasonable person would expect that disclosure to have taken place. That offence should have similar penalties as other offences in the act.

To further back up enforcement, I think the act should state that whistle-blower rights specifically apply where employees notify the Privacy Commissioner about a breach.

My second point deals with consent in the employment context. I have seen enough evidence through PIPEDA complaint investigations and Federal Court decisions to satisfy myself that the requirement for employment consent for new purposes that are reasonable ones in the workplace imposes a huge administrative burden on companies and can and does lead to situations where employees exercise a right to refuse consent in an arbitrary manner and for what are really justifiable information collection purposes.

The Alberta and B.C. laws foresaw this problem. They wisely removed the requirement that consent be required in the employment relationship, moving instead to a standard where purposes must be identifiable, and actually identified to the individual, and must be reasonable.

I've seen no evidence whatsoever to indicate that the Alberta and B.C. model does not work well or that any real privacy rights of employees are trampled as a result of this model.

I undertook a very detailed analysis of the consent issues in my written submission, which I hope you will take a look at.

My final comments deal with a matter that has not received very much attention so far, and that's the way in which the Public Safety Act, 2002, amended PIPEDA to permit private sector organizations to collect new information about customers or employees, or about any other party on their own for purposes related to national security, defence of Canada, and the conduct of international affairs, or to do so at the request of a national security agency.

In making these amendments, which were added in the wake of 9/11 and the heightened concern for public security, PIPEDA enters a very different sphere than normal commercial business activity. With these amendments, organizations can, on their own or at the prompting of a state, undertake the kind of information collection that is normally undertaken only by state agencies and where our society has recognized a need for the highest level of constitutional protections under the charter.

With these amendments, because they enable a business to collect new information about a person on the suspicion of a security threat or to do so at the request of the RCMP or other security agencies, there's a great risk that charter rights could easily be offended.

As you know, private businesses are not subject to the charter directly, and in some cases have very little knowledge or understanding that charter rights could therefore be trampled if they collect information in ways that would not be considered reasonable. Moreover, if private companies are co-opted by security agencies to collect such information on their behalf, there's also a further risk that such agencies could use PIPEDA to bypass or to do an end run on their charter obligations.

In my written submission I made the effort to explain in great detail the nature of my concerns. This is a complex issue. I hope you'll take the time to read these detailed comments and consider them carefully.

I must stress that I am not a lawyer and not schooled in the intricacies of constitutional law and charter rights. However, as a privacy consultant who studies the details of PIPEDA very carefully, I was struck the moment I saw these new Public Safety Act amendments that there was a grave and real risk that charter rights—first section 8 and possibly section 7—could be violated if such collections of information ever took place. As constitutionally protected rights are at issue here, I urge the committee as a matter of public duty to give this issue the attention it deserves, and I recommend that it report to Parliament that the government should reconsider these amendments with a view to removing them from the act.

● (0920)

Thank you for the opportunity to give you my comments. I must say, in closing, that as a privacy consultant I am constantly asked in training sessions all kinds of questions about the act, and I'd be glad to answer any question you've got about the act and how it works.

The Vice-Chair (Mr. David Tilson): Mr. Long, we appreciate someone with your expertise coming and giving us your thoughts. Thank you very much.

The Dominion of Canada General Insurance Company, Ms. MacKenzie and Ms. Bercovici. You have up to 10 minutes.

Ms. Ann MacKenzie (Privacy Officer, Dominion of Canada General Insurance Company): Hi.

Members of the committee, ladies and gentlemen, good morning.

I am Ann MacKenzie, privacy officer of the Dominion of Canada General Insurance Company. Presenting with me today is Vivian Bercovici. Until recently, Vivian was general counsel at the Dominion, and she continues to advise us in private practice. We appreciate the opportunity to present our views and concerns directly to this committee.

We have provided a booklet of materials to you, which includes our submissions made in September 2006 to the Office of the Privacy Commissioner regarding a statutory review. The bound material starts with our table of contents. It's followed by today's written submission. The tab materials that follow it support our written submission, and the French and English versions are separated by blue pages. The French translation of our oral presentation will be provided later, in a few days.

The Privacy Commissioner has provided this committee with a summary of submissions that can be found at tab 5 of our material. I note that certain positions put forward by the Dominion in our September 2006 submission to her do not appear to be reflected in the OPCC résumé. So today we intend to focus our comments on two issues: first, the matter of solicitor–client privilege, PIPEDA, and the recent Federal Court of Appeal decision in the Blood Tribe case; and secondly, the right of the respondent to appeal a complaint made to the Privacy Commissioner under PIPEDA.

Vivian will now present our position regarding the first issue, solicitor–client privilege and related issues.

Mrs. Vivian Bercovici (Counsel, Dominion of Canada General Insurance Company): Thank you.

The discussion of solicitor–client privilege in this PIPEDA context was focused very recently by the Federal Court of Appeal decision in Blood Tribe, which was given in October 2006. You'll find it at tab 8 of our material. I know this is a heavy booklet, but we thought it would be convenient to have everything in one place. I'm sure you've heard a lot about Blood Tribe up to now. We have been following these hearings, and we wanted to make some comments on some of the things that have been said, because solicitor–client privilege is so important.

This case, the Blood Tribe case, is really about the scope of power of the Privacy Commissioner and the manner in which that power is exercised. It's a case about considering what the statute allows explicitly and the limits of discretionary interpretation. To analyze these fundamental principles, we must consider the intent of Parliament in enacting PIPEDA. I'm going to direct you to page 2 of our written submission at the front of the booklet where it's set out, where we talk about the balance and the purpose of the statute, and you can read it at your leisure.

When Parliament intends to legislate an ombudsman-type adjudicative structure, as in PIPEDA, then I submit that's what Parliament does. When Parliament intends to grant more expansive powers, such as those we might find in an administrative tribunal with rule-making powers, then that's what Parliament does. When Parliament intends to require that material protected by solicitor–client privilege be disclosed, then that's what Parliament does. Parliament did not do this in PIPEDA, and we must presume that this was not a matter of inadvertence or an oversight. Parliament did not intend that the Privacy Commissioner should have the power to compel the production of solicitor–client privileged documents.

I take you to tab 8 of the booklet now. Writing for the bench in the Federal Court of Appeal decision in Blood Tribe, Mr. Justice Malone states—

● (0925)

The Vice-Chair (Mr. David Tilson): Which page is that?

Mrs. Vivian Bercovici: I'm sorry. That's in paragraph 14 on page 6 of tab 8, so just near the bottom.

The Vice-Chair (Mr. David Tilson): Thank you.

Mrs. Vivian Bercovici: So right at the bottom, it reads:

> the recent approach used by the Supreme Court of Canada suggests that if Parliament wished to create a power to compel privileged documents then express language must be used.

If I can just refer you to page 8 of the same case, paragraph 22, about two-thirds of the way down, after going through all of the relevant case law, the summary comment states:

> In short, the reason express language is required to abrogate solicitor-client privilege is because it is presumptively inviolate. The exception for solicitor-client privilege in PIPEDA is not what shelters privileged documents from disclosure. The law of privilege does that.

Ladies and gentlemen, solicitor-client privilege goes to the heart of the order and integrity of our system of justice. An individual or party in any proceeding must know with confidence that any communication with their solicitor will not be disclosed. This allows free and unthreatened communication between solicitor and client, which facilitates the preparation and execution of a full and vigorous defence.

The impact of qualifying solicitor-client privilege, which has anchored a common law tradition for centuries, would be seismic. Just to bring it home, I'd ask you to imagine the sudden and retroactive abrogation of executive privilege and the profound effect this would have on government. I suggest to you that the impact of the Privacy Commissioner's position regarding solicitor-client privilege would be no less dramatic.

It is of the utmost importance that power be clear and be interpreted clearly. It is of the utmost importance that the commissioner's discretion in interpreting powers be consistent with our legal practices and system.

The insurance industry receives many requests from plaintiffs' counsel. You've heard about this already from our friends from the IBC. Often when litigation is contemplated—sometimes after a claim has been filed—counsel seeks production under PIPEDA of documents to which they are not entitled under common law or pursuant to the rules of civil procedure. These documents are protected by either solicitor-client privilege, litigation privilege, or both.

● (0930)

The Vice-Chair (Mr. David Tilson): Could you wait one second?

Mrs. Vivian Bercovici: Sure.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Are these documents in English only, Mr. Chairman?

[*English*]

The Vice-Chair (Mr. David Tilson): We have a problem that maybe you can resolve. It has been pointed out by one of the committee members that the material you're referring to, the legal quotations, are only in English. At least the written part is only in English. Is that correct?

But it's fair for her to read in English.

So, Madam Lavallée, as long as the witness is saying it vocally to the committee, that's acceptable. Then it would be translated. Okay?

Proceed.

Mrs. Vivian Bercovici: My apologies.

The Vice-Chair (Mr. David Tilson): Madame Lavallée, do you have a point of order?

[*Translation*]

Mrs. Carole Lavallée: I simply want to point out that it is very difficult to follow your explanations because we do not have the text in French. Your words are being translated into French but when you refer to material drafted in English, it becomes impossible for us to follow.

[*English*]

The Vice-Chair (Mr. David Tilson): Thank you. That is a good point.

Perhaps because it's not translated, and you are referring to legal.... Judges talk funny sometimes, so perhaps you could go slowly when you're referring to quotations.

Thank you very much.

Mrs. Vivian Bercovici: Certainly.

I apologize for that, but it will be a relief that I'm not quoting any more from case law.

The Vice-Chair (Mr. David Tilson): Thank you.

I'm sorry to interrupt your train of thought, but we have to clarify these things.

Mrs. Vivian Bercovici: That's okay. It's a good thing I have written remarks.

I was just talking about the difficulty in the insurance context, because very often requests are made during the litigation process for privileged documents.

With respect, we submit that it was highly unlikely that Parliament intended an interpretation of PIPEDA that would permit the circumvention of privilege in this manner. Parliament would not have sanctioned this result.

We also have to ask, what happens if the commissioner finds that documents, which are the subject of a complaint, are not privileged or that they must be disclosed anyway? Then what?

Ann MacKenzie will address this issue with you.

Ms. Ann MacKenzie: Our interpretation of PIPEDA is that there is no clear right of appeal for the respondent to a PIPEDA complaint. This is raised in our September submission at tab 2, page 3, and in our current written submission at page 5—and our current written submission is translated into French, my apologies.

This issue that we're raising today wasn't raised in the commissioner's oral testimony before the committee, or in her written submission or the résumé of submissions received from third parties. We think it's very important that we should bring it to your attention.

Section 14 of PIPEDA allows the applicant to appeal a finding of the Privacy Commissioner to the Federal Court. There is no such explicit right of the respondent. We respectfully submit that this is a matter that should be corrected in this statutory review. The powers of the Privacy Commissioner are significant powers that may profoundly affect a commercial interest. To allow one party a right of appeal and to deny another party the same fundamental right or opportunity is inconsistent with the common law standards of fairness. We ask the committee to consider recommending to Parliament that the statute be amended to explicitly provide for a right of appeal for the respondent.

In addition, we ask this committee to consider addressing the current practice of the Privacy Commissioner regarding disclosure of complaints. Based on our experience, it seems that the identity of a complainant is not always disclosed to the respondent, nor is the complete original complaint. Rather, the respondent receives a paraphrase.

PIPEDA was intended to be a general guideline for a principled approach to the collection, use, and disclosure of personal information, not to create a parallel justice system. All Canadians would benefit from a clarification of the commissioner's powers, so that we understand with certainty and confidence the standards that are being applied.

In closing, on behalf of the Dominion, I wish to thank the committee for hearing us today and for indulging us. We commend the Privacy Commissioner and this committee for such careful consideration of the matters before us.

Thank you.

The Vice-Chair (Mr. David Tilson): Thank you very much.

You've all raised some excellent points, and I know members of the committee will have some questions for you.

The procedure is that we go in a round, and each caucus has up to seven minutes for questioning, including answers.

Mr. Pearson is first.

● (0935)

Mr. Glen Pearson (London North Centre, Lib.): I want to apologize for being late. I'm the newest member of Parliament here and I went to the wrong room.

I'm interested in your last few comments, Ms. MacKenzie, in that you want the respondent to be able to also have a right of appeal.

Can you tell me how that would look? For instance, a client does that. Therefore, a client has the right to appeal if they have any difficulties or if they feel some violation has taken place. How would a respondent do that? Who would do that in the case of a respondent?

Ms. Ann MacKenzie: You're describing a situation, for example, in which one of our policy holders complains to the commissioner. The commissioner makes a finding that we don't agree with. We would then like to have an opportunity to appeal through some formal process, appeal to the commissioner to review the decision and challenge it. Currently, I believe, it goes to the Federal Court, which is very cumbersome, but we would like that right of appeal as well. That would be commensurate with the applicant's rights.

Mr. Glen Pearson: It would be the same as the applicant.

Thank you.

The Vice-Chair (Mr. David Tilson): Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: In several presentations, in particular those of Mr. Long and Mr. Bundus, we were told that it was the insurer's duty to notify their client when there had been a privacy breach. As you know, clients must provide their insurance companies with information such as their social insurance number, but also personal information on matters such as their financial situation, their health, their mortgage, and so on. There is very little personal information that is not provided to the insurer. The information that is given to you is very significant.

It is your duty to notify the client—at the very least—but once a claimant has been informed, what happens next and what kind of protection can he avail himself of?

My question is for Mr. Long or Mr. Yakabuski.

Mr. Mark Yakabuski: Thank you very much, Ms. Lavallée.

As you know, consumers have a right to access their files and to correct any personal information that is incorrect.

That being said, we have pointed out today that a distinction must be made between personal information as such and work product information, which is entirely different.

Randy, would you like to expand on that?

[*English*]

Mr. Randy Bundus: I would add to that. If I understood your questions properly, your question was specifically what the client can do when they get the notification of the privacy breach.

It would be in the client's best interest to check all of their records to ensure that nothing untoward happened with, say, their banking statements or any of their financial or whatever kinds of records. The client should pursue the companies that had the breach occur, to get those companies to assist them in correcting whatever harm had happened to them.

It is a very serious matter to have losses of personal information. We in the insurance industry are very cognizant of that concern, and we take every effort in our industry to make sure it doesn't happen. But if it were to happen, it would behoove us as insurers, or as industry in general, to assist our customers, for good customer relations, to make sure we correct the wrong in whatever manner it takes to do so.

Mr. Murray Long: In my view, I think the onus should be even higher on companies, because they collected the information and they had the responsibility to safeguard it.

When a breach occurs, as a practical minimum standard if it involves financial information, the duty is not just to notify; the duty is to make sure the individual suffers no lingering harm as a result. It's hard to know whether this should be a standard put into the law or a standard that is encouraged by the Privacy Commissioner for adoption at a practical level, but certainly there should be an obligation on a company to make whole what has been lost. That goes to the heart of really dealing with the breach. If it was the company's fault, they should step up to the plate and they should be required to rectify any problems.

That includes things like the credit watch services. They should not be things people should have to go out and find on their own. Where you have a breach that could lead to identity theft or credit theft, you should have an obligation imposed on the company to actually pay for those kinds of credit watch services in order to make sure the individual has not suffered harm because of that breach.

● (0940)

[*Translation*]

Mrs. Carole Lavallée: Mr. Yakabuski, you spoke about witnesses in the case of accidents. If I understood correctly, you must obtain consent from the claimants or the victims before collecting statements from witnesses to an accident. Is that what you stated? Is that the current procedure?

Mr. Mark Yakabuski: We absolutely want the act to be amended so that it is clearly stated that there is no obligation to obtain consent from a third party before being able to speak to a witness. Sometimes that is absolutely impossible. We want a witness' statement to be considered as part of the witness' personal information. We want that to be clarified in the legislation so that these situations no longer occur.

Mrs. Carole Lavallée: Is it that the current requirements are not clear or is it that in order to collect a witness' statement, you are obliged to obtain the consent of the victim?

Mr. Mark Yakabuski: The current requirements are not clear and we simply want them to be clarified.

Mrs. Carole Lavallée: Has that prevented you from collecting statements from some witnesses?

Mr. Mark Yakabuski: It prevents us in that a person can tell us that we don't have the right to collect the statement. Obviously that can cause problems for many people, including the witnesses.

Mrs. Carole Lavallée: Could you give us any examples or is this simply a situation that you are afraid might occur? I'm trying to understand.

[*English*]

Ms. Ann MacKenzie: May I answer that question, as I actually work at an insurance company?

Yes, we do have examples of where that happens. For example, if someone is suing one of our policyholders for an injury claim and they're making allegations that our insured is at fault or caused a certain amount of damages, then if we have witnesses to the accident, we have had numerous cases in which the lawyers representing the person who is suing our policyholder, who we're required by law to defend, have said, “You've obtained witness statements, but you don't have my client's permission to do that, so you can't use them”, or, “You've done it inappropriately”. So we do have examples, because they happen quite frequently.

The Vice-Chair (Mr. David Tilson): Thank you.

Mr. Martin is next.

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

I have three areas I'd like to touch on. First of all, this duty of notification if a breach occurs is currently of great interest to Canadians, considering the Winners and CIBC incidents. It's huge.

In the context of that news, a lot of us, even those of us on this committee, don't realize that there are 30 million breaches per year in the U.S. There is no corresponding research in Canada, but if you take 10% of the population, you might be able to assume there are 3 million breaches of credit card information. That's not even touching on what other financial information may be held by other sectors, such as the insurance sector, and there is no duty to notify clients, although I do notice people are getting new credit cards in the mail this week. My own staff member got one today, and so have others I have talked to.

The credit companies are catching breaches and often fixing them with no injury to the client, but they are not telling us. I think I might change how I do business if I knew my card had been compromised one or three or seven times. I might change where I do business, etc. I have a right to know, I think.

You touched on that, but how do we tighten that up? In the U.S. there is a duty to notify in 32 states. Briefly, Mr. Long, do you recommend that Canada implement a hard and fast obligation to notify clients of any breaches?

● (0945)

Mr. Murray Long: I can address that first. I certainly agree with you, Mr. Martin, that we need to have some formal legal duty to notify built into the act. I think Canadians demand it, just to build trust in the electronic commerce world.

I don't necessarily recommend the U.S. approach; in that approach, most state laws are based upon the California model that was the first law. It's very binary, in the sense that if any one of certain specific elements is disclosed in an unencrypted form, you must notify.

I think David Loukidelis, who is watching this to see whether the model works or not, made the point when he was here that it could lead to tons of disclosure notices going out to people, and they become lost in the.... You get so many that you end up losing the impact.

I certainly think there needs to be a certain level of discretion given to business about when they notify, but it should be based upon objective standards, such as a reasonable person's standard, which is something on which the law is fairly clear. It's based, of course, upon the tort of negligence and the idea that reasonable persons must act in a prudent manner. It is something you could look at very objectively. I think the duty should be there so that if there is any breach whatsoever—not just of financial data, but of health information or anything else that is sensitive information—and a reasonable person would expect notification of it, then you must notify the public.

Mr. Pat Martin: That helps me segue into another issue I had.

Health information has just recently been added to the obligations here under PIPEDA. In 2002, I believe, the act was extended to cover health information. A lot of us, in reading about PIPEDA, seem to feel that it was hastily thrown together to comply with the European Union's demand that in order to trade e-commerce information, the nation you're trading with must put in place legislation comparable to the Europeans' data protection directive, which they implemented in 1995. They said if you're going to play ball with us, you have to have comparable, similar protection or we're not going to share information.

Well, in the province of Manitoba, the Tories sold the Manitoba health data services crown corporation to a private outfit. That private outfit then, of course, as private companies do, got sold to a company in Houston, Texas; that company got sold to a company in Denver, Colorado. My personal health information is now out of the country.

Do you know of any American protection, comparable and similar to the EU's data protection directive and Canada's PIPEDA, that would give me confidence that my health information isn't being sold to Pfizer so that they can crank out advertisements or something?

Mr. Murray Long: Mr. Martin, I actually checked into that story. I actually checked with the Manitoba ombudsman. I was very, very curious about your comment earlier that your health information was in the U.S.

I got total assurances that it never left the province. I was very interested in that story and I did some research into it because I write a thing called *Privacy Scan*, and I have been following these hearings and looking at the issues raised. Anyway, I'm glad to tell you that according to the ombudsman in the province—

Mr. Pat Martin: I'm somewhat relieved to know that—

Mr. Murray Long: —your data has not left the province.

Mr. Pat Martin: —although not from a political point of view, because I use that story a lot.

Mr. Murray Long: To the broader question about U.S laws, there are quite strong sectoral laws in the States involving health information, banking information, and other specific areas, such as children's privacy, but no general, broad federal-level encompassing privacy act. There are tons of state-level laws.

Mr. Pat Martin: How do they trade with the EU, then? The EU demands parallel protection.

Mr. Murray Long: Through the Department of Commerce, they created something called the "safe harbour" arrangement. Companies voluntarily enter it, and when they do so, they declare that they will abide by a set of privacy rules. Because they're declaring that, they are subject to the Federal Trade Commission Act, which prevents misleading and deceptive advertising. If you say that you adhere to the safe harbour rules and you don't, then the Federal Trade Commission has the power to investigate you and charge you. There are very substantive penalties for companies that breach their declared statements about privacy.

● (0950)

Mr. Pat Martin: That's very interesting.

Ms. Ann MacKenzie: Mr. Martin, I would like to add that, in the property and casualty insurance context, insurers are also required by the Office of the Superintendent of Financial Institutions, the OSFI.... They have very stringent guidelines on outsourcing that we must follow that would provide protections for that situation in the property and casualty realm.

I'm hoping that someone will ask me a question about the duty to notify, since I'm the only actual privacy officer here.

The Vice-Chair (Mr. David Tilson): Maybe the next round, Ms. MacKenzie.

Mr. Wallace.

Mr. Mike Wallace (Burlington, CPC): Well, that sets me up, doesn't it? I'll try to get back to you.

I do want to talk to you about the Blood Tribe issue, and I want to be clear so that I understand it. Actually, I think we've only talked about it at one other meeting. I'm not sure it's been a primary piece here.

It went to Federal Court and the Federal Court overruled the province on it. Is that not correct? The Federal Court actually supports your position that the commissioner's power cannot overrule the solicitor-client privilege. Is that not correct?

Ms. Ann MacKenzie: Yes, it is, and I'm going to ask Ms. Bercovici to explain that. I'm not bragging, but I'm not a lawyer either.

Mrs. Vivian Bercovici: It was the Federal Court, Trial Division, that said, "Sure, Commissioner, you're right, you interpreted your powers correctly and you may require production of solicitor-client privilege documents", which was a finding that is really quite inconsistent with the common law—

Mr. Mike Wallace: Right, so it was appealed.

Mrs. Vivian Bercovici: —and the Supreme Court of Canada. It was appealed to the Federal Court of Appeal. The Federal Court of Appeal is the decision at tab 8, which you have.

My understanding, from the transcript of when the commissioner appeared, is that the Privacy Commissioner has sought leave to appeal this decision to the Supreme Court of Canada. We don't know yet whether leave to appeal will be granted. So this is the law that now stands. It was something that she discussed in her comments before the committee. Notwithstanding the fact that it may not have been raised many times other than that, it is a terribly important issue.

Mr. Mike Wallace: Based on the current Federal Court of Appeal decision and the legislation, as it's written, the solicitor-client privilege is protected based on those decisions.

Mrs. Vivian Bercovici: That's correct.

Mr. Mike Wallace: Okay, I just want to be clear on that.

I will give you a shot at notification, if you'd like, Ms. MacKenzie. Would you like...?

Ms. Ann MacKenzie: Oh, sorry. I apologize for being slow in picking up.

I did want to say that as a privacy officer I actually work.... The Dominion of Canada has not had a breach, but I would caution against being too prescriptive about notification and the procedures. I'm going to make an analogy. This is a lot like when insurance companies have to deal with a catastrophe client. You can set out generally the steps that you want to follow in order to contain, evaluate, determine the impact, decide whether you want to notify your clients, and then prevent future things, but you can't be too prescriptive about it. Otherwise, you're going to miss the opportunity to actually address your policyholders' concerns.

I also want to say that insurance companies already have a duty of utmost good faith to deal with our policyholders. We believe that we already have a responsibility to appropriately notify our clients and assist them, if there's anything we've done, to rectify the situation.

We support the IBC's position on notification, which is set out in their submissions. But in terms of requiring notification, there has to be a threshold. It has to be based on some reasonableness, and it has to be to the client and not to some administrative tribunal.

Mr. Mike Wallace: Mr. Long, I'm going to ask you a question based on the presentation from the Dominion of Canada group. They would like to see us add in section 14 that the respondent be able to appeal to the Federal Court. Do you have any comments on that?

Mr. Murray Long: It's already happened. There has been at least one case where a respondent won the right to have a judicial review of a finding made by the Privacy Commissioner's office. It's already entering the common law realm in that sense.

I have no difficulty with it. I think there are situations, but they're going to be rare ones. There will be situations where organizations feel strongly that their position has not been well represented or there has been some injustice done to them. Keep in mind that these are only recommendations and they're not binding orders.

I was quite surprised that one organization would actually go to the Federal Court to challenge what was not a formal binding order but only recommendations. They did so, and they won the right at the Federal Court to have the application heard.

I think it creates a balancing of interests in the law, and I don't see a huge harm coming from that. It'll be rarely used.

● (0955)

Mr. Mike Wallace: I have a question for the Insurance Bureau group. In your submission you talk about requests from individuals who are suing companies and their ability to say no, you can't have your own private information. Is that actually happening? Are people doing that? Are they winning those requests?

Mr. Randy Bundus: I would say it is frequently happening. I'm sure Ann will be able to confirm that, being closer to the company front, where it does happen.

Our argument is that they will have the ability to access that kind of information through the court processes. Once it's in litigation, there are procedures in place to protect both parties. They were designed over years and years of courts analyzing these kinds of issues.

To override these civil procedures that are currently in place, because a request has been advanced under PIPEDA, strikes us to be —

Mr. Mike Wallace: I want to know this. Is it happening? Are they successful in getting their private information?

Ms. Ann MacKenzie: It is happening. We are being asked by plaintiffs' counsel, by lawyers who are representing people who are suing our clients. They have made access requests for the information. We have no trouble giving them the information. We are saying that documents subject to solicitor-client privilege should remain under solicitor-client privilege.

This gets to our point about the respondent's right to appeal a decision, because it shouldn't happen. It should be clearly set out in the statute and should not be ambiguous or something that happens along the way. It should be clear.

We have also seen privacy commissioners' findings that, despite the Blood Tribe case, still continue to say yes, you have to hand over the documents. They'll decide whether it's privileged or not and then release them.

Mr. Mike Wallace: Does the judge decide?

Ms. Ann MacKenzie: No, the privacy commissioners decide.

Mr. Mike Wallace: The Privacy Commissioner decides.

Ms. Ann MacKenzie: We take issue with that.

I can cite one particular case that I'm dealing with right now, where we've already made full production in the civil proceedings. Full production is very prescribed and you have to set out everything. You have to say what you have and what you don't have. It's still being challenged. The Privacy Commissioner's office is still saying they want to see the full file and they'll decide.

The Vice-Chair (Mr. David Tilson): Thank you, Mr. Wallace.

Mr. Mike Wallace: Thank you, Mr. Chairman.

The Vice-Chair (Mr. David Tilson): That concludes the first round of seven minutes.

We'll now proceed with five-minute rounds.

Not as a member of this committee but as an individual, I must say that I agree with Ms. Bercovici on what she said about solicitor-client privilege. I've seen the withering away of solicitor-client privilege with the former Information Commissioner and I see it with the Privacy Commissioner.

This question is either to Ms. MacKenzie, Mr. Bundus, or to you, Ms. Bercovici, on the issue about the statements of witnesses.

It is almost as if you are suggesting that insurance companies should be privileged. It could be a criminal investigation or a highway traffic investigation. For example, for the police, for a crown attorney, or even for civil matters, you are suggesting those statements should not be allowed to be brought to be subpoenaed. Is that what you are suggesting?

I'm looking at Ms. MacKenzie or Mr. Bundus.

Ms. Ann MacKenzie: We're not saying that, no. We're not saying they shouldn't be subject to subpoena, that they should be privileged. We're just saying we shouldn't be prevented from defending our clients and carrying out our legal obligations under the policy by not being allowed to talk to a witness.

● (1000)

The Vice-Chair (Mr. David Tilson): Just so I'm clear, if there was an information application, those documents would not have to be produced, but if they were subpoenaed they, would have to be produced.

Is that what you're saying?

Ms. Ann MacKenzie: I don't understand—

Mr. Mark Yakabuski: I think they're two different issues, with all due respect, Mr. Chairman. What we're saying is that the law is not clear with respect to witnesses' statements currently. We're saying that we ought to have the right to go to someone who's been a witness to an accident and to get their testimony and not be encumbered by another party who says you have to get their consent in order to talk to this person who was directly a witness to this accident.

In other words, we're saying if you're a witness to an accident, your testimony is your personal information. It's your right to give it to the insurance company if you feel so inclined. We ought not to have to go to someone else to get their consent first. That's the issue there, and it needs to be clarified in the law.

The Vice-Chair (Mr. David Tilson): Okay.

Mr. Stanton.

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chairman, and thank you to our panel this morning.

It's a very interesting take on a few very key issues for an important industry, in the case of the insurance industry. And thank you to Mr. Long for your insights this morning as well.

I'd like to direct my first question to Mr. Yakabuski.

This is specifically on the area of work product. You spent some time on that, and you said that in the current PIPEDA legislation, it is an inhibitor of innovation, research, and so on. Using the notes that were supplied to me by the Dominion of Canada—thank you very much—I was able to find the Privacy Commissioner's comments on that topic of work product.

She appreciates the fact that this is a complex area, but raises some concerns that if we go for a complete blanket exemption of work product information with respect to PIPEDA, it raises the spectre of, for example, video surveillance in the workplace, that type of information. What prevents that from falling into the realm of personal information? That's one issue. I wonder if you could perhaps address the Privacy Commissioner's concerns in that regard.

Secondly, you mention that there is an ability to draw a line, in fact, between when the information regarding an employee—in this case—is personal information and when it's work product. Can you just give us an example of how that might work?

Mr. Mark Yakabuski: I'll let Randy talk a bit further, but let me just say that we're simply saying that this has worked extremely well in the British Columbia legislation. We're asking for nothing else but the dispositions that are now in the B.C. legislation. I think they will work federally as well.

I think it's very clear that we are not talking about employee information. If there's information about an employee, that's personal information. What we are talking about is all kinds of statistics that businesses generate about the products and services they provide. If you want to have a competitive economy, you have to make sure that is out there in the public domain, accessible, so we can have companies that learn from successes, build on those, and improve their products and services. Otherwise, you're going to potentially be creating a bunch of oligopolies in this country.

From an economic policy point of view, it is fundamental that information about a company's products and services generated in the course of doing business be accessible and not be considered personal information.

I draw a totally stark distinction between that and the employee information that the commissioner might be referring to.

Mr. Murray Long: May I jump in on this one?

I've thought about those comments by Jennifer Stoddart at some length, and I think you can draw a fairly bright line between a definition of work product information as work output and work processes, but it would not include video monitoring or video surveillance.

I don't think her concerns in this particular case are realistic ones. I don't want to put words in her mouth, but I honestly have tried to assess that. I think it is useful, certainly, to add a definition of work product in the act, just to provide clarity for the business marketplace. I think if you work with the B.C. definition, it is such that it is not going to incorporate or include things like video surveillance. I think you can make that kind of distinction fairly clearly.

● (1005)

Mr. Bruce Stanton: Do I have any more time, Mr. Chairman?

The Vice-Chair (Mr. David Tilson): One minute.

Mr. Bruce Stanton: There is just one item for Mr. Long.

Mr. Long, you raised the whole issue of the Public Safety Act amendments and the potential threat these have to charter rights. You spoke of them in terms of being potentially offending. Could you cite some examples or some circumstances that you see, in plain terms, where that threat exists? Would you go over, just for the record, where the potential problem is there?

Mr. Murray Long: Sure. The act currently authorizes businesses to use information they come across in the normal course of their business activities. So if a business organization saw something it thought was suspicious in nature, it could certainly use that and later on disclose that to the RCMP or to CSIS or whatever.

What the law has done now with the Public Safety Act amendment is it has expanded that to allow a business organization to collect information, and the word "collect" in my reference point means something you don't already have. So you can go forth and gather new information for the purpose of later disclosing it to the RCMP. I think the fact that the law has now permitted organizations and private businesses, on their own, without direction, without guidance, to start collecting new information about employees or their clients or any third party certainly creates a situation where they could easy violate charter rights in the sense of perhaps engaging in things that would be considered an unreasonable search. For example, a company could decide, on the basis of its own suspicions, to do a locker search of employees because they're concerned about some national security issue. I think the law should not permit private businesses to start collecting new information for this purpose on a suspicion basis. There's a pretty low bound in terms of the anti-terrorism type of investigation. It's not even probable cause. It's a suspicion of, and I think there is certainly a concern.

Secondly, if the RCMP came to a business and said, we'd like you to collect information for us, they're really making that business an agent of the state, and they may do so in circumstances where they would not themselves be able to get a warrant, but they're going to ask the business to collect information for them. I can't say for certain that this has ever occurred, but it's certainly a troublesome area of the law, and I certainly think you need to look at it and you need to recommend back to Parliament that these amendments need to be reconsidered, at the very least.

The Vice-Chair (Mr. David Tilson): Thank you.

Mr. Vincent.

[*Translation*]

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

Mr. Yakabuski, thank you for coming today. I read your brief closely. I believe Mr. Bundus is the one who wrote it. I'm sure your employer is very pleased with what it contains. Let's begin with your first point, dealing with the work product.

Page 4 of your brief states:

> "Work product" is not personal information because it does not relate to an identifiable individual; instead, it is proprietary business information that belongs to the organization. For example, an insurance company's strategy on handling a specific claim is not personal information as it is not information about an identifiable individual; [...]

You meet with the witness in order to take this statement, and then you meet with the client or the individual who has been wronged and you tell that individual that a witness has made certain statements. However, that does not count as information about an identifiable individual because it is simply a witness' statement. Therefore you can say anything to the insured, including that you have overwhelming evidence against them but you are not in a position to disclose your source of information.

You are the one who decides, because this is information that will influence how the insurer deals with the claim. Whether the case goes before the courts or not, you are under no obligation to disclose your sources. However, if the case does go before the courts, then you are obliged to disclose your sources. That's my first point.

Second, in the same document, on the next page, you go even further. You talk about the insured's medical files. Let's say, for example, that the claimant has an accident and you decide to go looking in their medical files in order to find out whether or not there had ever been anything physically wrong with that individual in the past. This is what your document states:

> "An individual prescription, though potentially revealing about a patient, is not in any meaningful sense about the prescribing physician as an individual. Rather, it is about the professional process that led to its issuance and should be regarded as a work product—that is, the tangible result of the physician work activity."

If I have understood correctly, this means that you can meet with the physician and request a list of all the prescriptions that the client has ever been given, and that this list will not be considered as personal information because the physician provided it during the course of the physician's work activity.

Let's go little further. You refer frequently to British Columbia and Alberta; there are not many references to Quebec in your brief. This is what it says:

> The effect of these provisions in the B.C. PIPA is that "work product" information is not accessible by an individual. We agree with this sensible and reasonable approach.

Except medical information, if I understand correctly! I would like to hear further explanations on your brief's proposal. It states:

> A definition of "work product", which includes the work documents of an employee or business person that were generated in the course of the employee's or business person's work, [...]

● (1010)

Mr. Mark Yakabuski: Mr. Vincent, let us not confuse things.

First of all, a witness statement is something entirely separate. We are asking that the law be clarified so that an insurance company or another party has the right to speak to you directly if you have been witness to an accident. Only at that point would what you have to say be considered your own private information. We want the law to be clarified. This is entirely separate.

Secondly, when we talk about work product information, we obviously consider that personal information is sacred. Obviously, you or I are entitled to our personal information. It is up to the commissioner to decide on this.

All we want is for the bill to recognize that some information is not personal and relates to work-product information, whether it is the work product of an insurance company, the local corner store, or a large automobile manufacturer.

Let us not confuse things. We simply want to make sure that by applying the protection of the Privacy Act, we are not killing the Canadian economy.

Mr. Robert Vincent: My question relates to the fact that in your documents, you include—

[*English*]

The Vice-Chair (Mr. David Tilson): You'll have to wait for another round, since you're time is up.

Mr. Van Kesteren.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you, Mr. Chair. Thank you all for coming here as well.

This has been a very interesting and informative session. It seems as though each one becomes much more interesting and much more informed.

I'm rather being kind. I don't want to be unkind, but I guess what I'm trying to say is that we see the complexity of this act and this bill. When I was first elected, I had the good fortune of sitting with Ms. Stoddart at a meal. She introduced herself, and I thought, "Privacy? That's interesting; I've never heard of it before." If there are 33 million people in Canada, probably 32.999 million or whatever have never heard of it either.

As a matter of fact, I remember talking to one of the parliamentarians who came here to one of the meetings; he'd been here a little longer than I, and he was surprised and had never heard of it either. I don't know whether it was of the Privacy Commissioner, but of one of the commissioners.

The point I'm trying to make, and I made this statement to some of you and publicly made it at the last meeting too, is that I really believe the insurance industry and the banking industry could write the book on privacy. I think you do a good job and I believe it's in your best interests to do a good job.

What's beginning to happen, though, as I view this whole process, is that the average guy on the street.... Before I was a parliamentarian, I was a businessman, and I commend you for your work, but if I got a brief like that talking about privacy, I would have the living daylights scared out of me.

I think the complexity is getting to the point now where, aside from the banks, the insurance companies, and possibly major manufacturers such as Zellers and Wal-Mart and such, the bill is getting way over our heads. We're getting into waters that I don't know if we want to tread. It is for that reason that I liked the recommendation that we leave things the way they are.

Is there a way we can get around this? Is there a way that possibly the industries I've mentioned, and whoever else it would pertain to, could move in those areas and leave the rest of us alone, or do we all need to be dragged along with this current of complexity?

I leave that open to anybody.

● (1015)

Mr. Murray Long: Hopefully, sir, the changes will simplify the act and make it easier for small business to use. Some of the recommendations I've seen made over the past number of meetings here have indicated to me that if they were put in place, they would make it easier for the small business sector. I think that's an important point.

Secondly, there's the really critical issue of small business education. That, in my view, hasn't happened effectively yet. There's an urgency for the Privacy Commissioner—and the private sector as well, through different associations, organizations, and so on—to spend more effort trying to educate small business about the fundamentals of the law.

In most cases, if you're not collecting a lot of sensitive information, the law can be fairly simple to understand and apply. It looks complex on paper, but for small business it comes down to very simple rules. The problem is that there hasn't been enough education yet to explain those very simple rules to the small-business person. If that happens, you'll solve a lot of those problems.

But we need to make modifications to the statute itself to make it easier for business and for the public as well.

Mr. Dave Van Kesteren: I want to follow that. You say "hopefully", and that's a great word, but I'm a little suspicious about it. I want somebody else to grab this too. I want to go back to the point about whether it is possible that this act can be directed on a broad level, so that the average person who's—

Ms. Ann MacKenzie: There are a couple of things, and I'd like Vivian to expand on this a little bit.

One thing I will say is that in terms of customers—I'm not addressing small business, but speaking in terms of our customers—I'm also the ombudsman for Dominion. Every complaint or concern comes to me, and we don't expect our policyholders to articulate their complaints in legislative style. If they have a concern, no matter how inarticulate, or are not even sure what the complaint is, our job is to help them out.

But concerning legislative complexity, I would like Vivian to expand a bit to help answer that question.

Mrs. Vivian Bercovici: I will be brief in my comments, but if I may.... I know that's an oxymoron—a brief lawyer—but I'll do it.

The Vice-Chair (Mr. David Tilson): You'll have to be brief.

Mrs. Vivian Bercovici: Thank you.

I agree with you. I think that when you have an omnibus statute like this that purports to deal with a single-person enterprise in an insurance company—because it does apply to all commercial enterprise—I think it's very challenging, if not impossible, to have it work effectively.

You know, this is a statement of principles. It was intended to bring attention to the fact that information was being distributed electronically with absolutely no controls. So it introduced this recognition of ownership and interest in private information.

It may be more appropriate to leave this statute as a statement of principle and look to specific statutes, such as those that regulate our sectors—the Bank Act, the Insurance Companies Act—where you have government officials who are very expert in the particular issues and where it is very complex. And it may be more appropriate to delegate these sorts of issues, in detail, to those sectors. It's good business, and I think it is being done in various sectors.

The Vice-Chair (Mr. David Tilson): Thank you.

We'll go to Mr. Martin.

[*Translation*]

Mrs. Carole Lavallée: I believe that it is my turn.

[*English*]

The Vice-Chair (Mr. David Tilson): Your turn hasn't come yet. You're on here, but you have a ways to go.

[*Translation*]

Mrs. Carole Lavallée: Aren't you following the usual order?

[*English*]

The Vice-Chair (Mr. David Tilson): Your turn is not on, under the rules. I'm following the rules of the committee.

Mr. Martin.

Mr. Pat Martin: So do I have the floor, Mr. Chair?

The Vice-Chair (Mr. David Tilson): You do have the floor.

[*Translation*]

Mrs. Carole Lavallée: Excuse me, Mr. Chair, I do not understand that rule. Can you please explain it to me?

[*English*]

The Vice-Chair (Mr. David Tilson): A point of order.

The rule is that there is a five-minute round for each caucus. The second round goes Liberal, Conservative, Bloc, Conservative, New Democratic Party, Liberal, Conservative. You get one shot, and therefore you'll have to wait until the third round. The NDP and the Bloc only get one shot. The Liberals and Conservatives, because of their size in the House, get more shots than you or the NDP.

Mr. Martin.

● (1020)

Mr. Pat Martin: Thank you, Mr. Chair. I hope that doesn't go against the little amount of time we get.

The Vice-Chair (Mr. David Tilson): The New Democratic Party and the Bloc do an excellent job, Mr. Martin.

Mr. Pat Martin: Thank you.

Mr. Chairman, I'd like to take advantage of some of the experience on the committee to ask a question that's a bit outside the study today. The House of Commons is currently looking at Bill C-31, amendments to the Canada Elections Act. Part of this is requiring more identification for voters when they come to the voting station —

An hon. member: [*Inaudible—Editor*]

The Vice-Chair (Mr. David Tilson): Your time is not up. I don't want to take away from your presentation.

Mr. Pat Martin: No, I appreciate that. This is probably something we could talk about at a planning committee meeting, or one of those meetings where we talk about the structure.

The Vice-Chair (Mr. David Tilson): Madame Lavallée, I'd like some order, please.

Mr. Martin, proceed.

Mr. Pat Martin: Thank you.

Bill C-31 talks about voter ID, having to produce two pieces of ID, but it also would change the permanent voters lists. It would now have your name, your address, your phone number, and your date of birth. Now, in election campaigns that I've managed—four of them now—I've had 400 volunteers. And quite often you tear off a page of the voters list and say, "Go phone these 50 people and see if they'll vote for us." I'm wondering if all of you, as privacy experts, see it as a problem to be spreading the name, address, phone number, and date of birth of every Canadian to virtually anybody who wants it, and if that's not a recipe for identity theft.

Mr. Murray Long: I was surprised when I saw that bill and looked at the fact that the list would have date of birth on it. I think that's certainly the one element I would have a concern about, because it's certainly a piece of information that is much more personal than any other. Your telephone number is not particularly sensitive information, unless it's an unlisted number. But date of birth certainly is, and I would certainly not be very supportive of that being included on lists that are made available to large numbers of individuals.

Mr. Pat Martin: Does anyone else have any views on that? I know that's not why you're here. I thought I'd just take advantage of the expertise.

I do have a question regarding, specifically, PIPEDA. I know that in the province of Quebec, their private sector privacy legislation says that a business cannot transfer personal information to a third party outside Quebec unless it believes that the information will benefit from protections similar to what it enjoys within Quebec. That's a recommendation I would support, though. Maybe I missed it in your presentations. Is it a recommendation of your respective organizations that Canada should have comparable mention within PIPEDA?

Ms. Ann MacKenzie: Mr. Martin, are you talking about transborder flows of information within Canada or outside of Canada?

Mr. Pat Martin: I'm thinking about outside of Canada, much like the European Union has stated that they want their trading partners to have comparable.... The Province of Quebec has that very language. I notice a number of advocacy groups have been saying that Canada should do what Quebec has done.

Ms. Ann MacKenzie: I'll clarify a couple of things. Within Canada, just as a business practice, if we're doing business in Quebec, British Columbia, or wherever, we meet the highest standards, not the lowest.

Mr. Pat Martin: Which has the highest?

Ms. Ann MacKenzie: That is interesting, because it depends. In some respects Quebec does, in some respects Ontario does, and in some respects B.C. does. We pick and choose whatever is best for our customers.

As far as transborder flows of information, I touched on that briefly earlier when I talked about OSFI regulations for outsourcing. Perhaps Mark can speak to that more precisely than me.

Mr. Mark Yakabuski: I simply want to add that all insurance companies in Canada that are federally incorporated are subject to the Office of the Superintendent of Financial Institutions. There are very strict regulations on transfer of information outside of Canada. It is permissible, but it is reviewed by OSFI. It is important that it be allowed, because this is a very international business.

You have to understand that a very large portion of the capital that comes to provide insurance to homes, businesses, and automobiles in this country is provided from outside of Canada. So there is obviously going to have to be some transfer of information. I can assure you that this is highly regulated already.

● (1025)

Mr. Pat Martin: But is it statutory? Do you recommend that it be under PIPEDA?

Mr. Mark Yakabuski: No. I believe it is more properly regulated by the Superintendent of Financial Institutions, which is where it is currently regulated. They have the expertise in financial transactions, and I think that's where it should reside.

Mr. Murray Long: PIPEDA, of course, applies to all business organizations, not just those in certain sectors like insurance. I think the Quebec amendment was useful. It brought their law up to a higher standard, for sure. PIPEDA already has that standard to a certain extent. When you are transferring data for processing anywhere, whether it's to another province or outside the country, you have an obligation to put in place safeguards, including contract-type safeguards, that will protect the information.

On top of that, the Privacy Commissioner has offered a lot more detailed guidance on what she thinks should be required of organizations. Even if this does not get into the statute, there will be strong guidelines provided to the business sector on what constitutes reasonable safeguards when data is being transferred to another country for processing. So I think we're going to be bringing PIPEDA up to the Quebec standard through those kinds of mechanisms.

The Vice-Chair (Mr. David Tilson): Thank you.

Mr. Dhaliwal.

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

Thank you to the panel for coming out.

Reading through the presentation made by the Insurance Bureau of Canada, you make the very strong statement that if you don't have access to this work product, Canadians will be losers. On the other hand, you are saying that by work product information you mean information that's created by a company—by employees in the course of their business activities.

Could you clearly distinguish what you would call work done? You are also collecting names and ages, and getting all the information.

Mr. Mark Yakabuski: That's not what we mean by work product information. I think personal information is clearly defined in the legislation as information that relates to an identifiable individual. There are all kinds of other pieces of information that do not permit you to identify the individual.

I'll give you an example of what we're talking about. Let's take the health care industry. It's very important for lots of businesses out there to be able to have access to information that says they're seeing this number of patients in the system; this is the average cost of the services that are being provided; these services are being provided in these geographical locations. That's important for them to be able to build better services, improve services, and—I want to just answer Mr. Van Kesteren's question—this is more important than ever to small business in this country.

I'll tell you, if you don't distinguish work product information, and if the commissioner tells us some day that we can't have work product information—because her latest statement is along those lines—you are going to be shutting down access to small businesses all over the country that want to know what the big guys are doing so that they can compete better against them. That's essentially what it is. It's information that is not identifiable. It is commercial information and it is information that other actors in the economy need to be able to create, innovate, and improve products and services. We don't believe you should use privacy legislation to restrict that type of access.

Now the flip side of the coin, because there are two sides of the coin, is that when someone says, “I want access to my personal file”, of course we'll give them the file that contains their personal information. But what we're saying is that this file shouldn't contain the work product information that has nothing to do with that identifiable individual.

Those are the two sides of the coin, and I really think it is fundamental for a competitive economy in Canada that we make that distinction. If there's one change you make with this legislation, that's the one I'd recommend.

● (1030)

Mr. Sukh Dhaliwal: Do you see any negative impacts on individuals? In fact, this is very useful for the businesses, the small businesses in particular, but is there a negative impact on the individuals or on the clientele?

Mr. Mark Yakabuski: There might be a negative impact on some and a positive impact on others. If I'm a small business and I'm able to get access to work product information, say I'm a real estate broker and I want to grow my business, I want to know where the houses have been selling in Toronto or Victoria or somewhere else, and I might be able to build my business. Maybe someone else will be selling fewer houses because I'm selling more.

There are always some negative consequences, but these are the consequences that you would expect in a competitive economy.

Mr. Sukh Dhaliwal: You say that the person should have access to the file and that right now in the act it says companies should be charging the minimal fees. On the other hand, you say that companies should be charging reasonable fees for that access to information. How would you distinguish between reasonable fees and minimal fees? What would be the criteria? This is with respect to page 13 of your presentation to the House of Commons.

Mr. Randy Bundus: I'll attempt to answer that one.

The concept of the minimal fee may mean that you would have to put a less experienced person to prepare the response, whereas a reasonable fee is the fee that reflects the resources the company has to put internally to develop that response.

The example we would give is for insurance files. There is oftentimes a lot of documentation. Some of it is work product of the insurer. Other aspects of the insurance claims file is the personal information. To have a minimal cost, you'd put a very junior person without the experience to do that analysis, and they would get it all mixed up. Therefore, you have to have the right level of expertise internally assigned to that task. That right level of expertise will have perhaps a higher cost than the minimal cost that the insurer could do, but they have to do it right. Therefore, the reasonable cost is the cost of getting the right expertise to do the job to assemble the information to respond to the request.

The Vice-Chair (Mr. David Tilson): Thank you, Mr. Bundus.

Mr. Stanton.

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

I want to go back, Mr. Yakabuski, if I can, on this question of work product, because we've talked around it. I'll first say that I don't in any way disagree with your contention that this is an important aspect for research, for understanding products, and for marketing. Coming from the small business sector, I can tell you these are very important measures that often the small business sector could not get access to were it not for the ability of larger industry associations, for example, to be able to crunch these numbers.

My point of view is simply to get to the essence of how we achieve that correct balance. Again, revisiting the Privacy Commissioner's own suggestions on this...well, let me first go to your example. In your presentation, you cite, for example, in the case of vehicle repairs—if I can get it correctly here—"...effectiveness of billions of dollars of vehicle repairs we pay for each year, so that we can improve the service provided to our customers". How is it that PIPEDA would prevent that information from being disclosed now?

Mr. Mark Yakabuski: Well, when there wasn't a clear distinction between personal information and work product information.... Take a garage, for example, that contributes to one of a few databases available in the industry. They'll submit that this was the repair they did, the time it took to do it, the cost of the repair, etc.—a lot of information like that. These databases are available. Everybody in the industry uses them. They take that work product information and use them, as I say, to improve their own products and services. Now if that garage owner didn't want to give his competitors a chance to do as well as he was doing and he said that this is personal information and he's not providing it to anyone, I think we'd all be losers. That's potentially what we're facing by not defining work product information as distinct from personal information.

I can give you a million other examples of where you have a provider of a service who says he is not going to give the information about how many patients he saw today, where he saw them, and what the cost of those services were.

● (1035)

Mr. Bruce Stanton: With respect to the example you cited, and it's a good example, I must say, wouldn't that be more the decision of the company itself, say, if it's a member of an association that shares that type of information for its own purposes?

Mr. Mark Yakabuski: In business, as you know, you're probably submitting information in a myriad of ways every day of the week. If you were to submit that information to some organization and said that it's personal information and you don't want that released to absolutely anybody, you shut these things down.

Mr. Bruce Stanton: The Privacy Commissioner, in her decision in finding 14—and this is contained in your brief as well—certainly contends "that the meaning of 'personal information', though broad, is not so broad as to encompass all information associated with an individual". She goes on to say, "An individual prescription, though potentially revealing about a patient, is not any meaningful sense about the prescribing physician as an individual". It's talking about the professional process. There seems to be an agreement there that this type of information should in fact be available for the reasons you and your industry espouse.

I would say, again, where do we need to make this more ironclad?

Mr. Mark Yakabuski: I appreciate the commissioner's remarks; they're in our own brief. The fact is that the previous commissioner had a different view of work product information, and this kind of uncertainty is not good for the Canadian economy. I believe it is incumbent on this House to make that clear, that work product information ought to be accessible to everyone for the benefit of improving and innovating products and services in this country. It's the uncertainty that is unproductive.

I know everyone is well meaning; we're not in any way saying otherwise. But we are saying that this question is important enough that it should be clarified in law such that all companies and individuals in Canada have the certainty that this information—work product information only—will be accessible.

The Vice-Chair (Mr. David Tilson): Thank you.

Madame Lavallée, you have the floor.

[*Translation*]

Mrs. Carole Lavallée: Thank you very much.

My first question is for Mr. Yakabuski, who represents the Insurance Bureau of Canada.

Your written submission contains something that worries me considerably. The passage is on page 11 of the French document. Unfortunately, I do not know what page it is on in the English version. Your proposal reads:

> The responsibility of an organization to notify affected individuals of a privacy breach is a sound business practice and does not need to be included in the PIPEDA.

You understand that if we were to always rely only on what is considered sound business practices, there would be no law. That is why I do not agree with your proposal.

You call this a proposal, but really you're stating a principle. I find this to be rather peculiar, even more so because it would seem to me that an insurance company holds a lot of personal information on an individual. An insurance company is the kind of company that holds the most personal information on one's financial health as well as physical health. As such, insurance companies have more responsibilities than any other type of business. Nothing would be better than to legislate these responsibilities to make sure that everyone complies.

I must point out that the current legislation does not provide that those who are found to be in violation of the law will automatically be identified. When I found out about this, I was just floored. I do not understand why we would protect offenders and hand over discretion to the commissioner to decide whether the names of those who are found to be in breach of the law should be disclosed publicly.

In my opinion, the responsibility of a company is not only to advise its clients when personal information has been stolen, which may concern them, but also to make amends, as Mr. Long was saying earlier. I would like Mr. Long to elaborate on that subject.

Usually, such a letter is rather vague. The insurance company informs an individual that personal information has been stolen, that his or her information may have been included, and that out of the great kindness of the company's heart, it was considered that the client should be informed; and that's it.

The recipient of the letter does not know exactly what information has been stolen, what steps to take, what recourse he may have. To my mind, the company is responsible for our personal information. The company is not only responsible for providing us with the details, but also for making restitution.

Mr. Yakabuski, or Mr. Long, I don't know if you wish to comment.

● (1040)

Mr. Mark Yakabuski: With great pleasure, Madam.

In turn, I wish to ask you a question. How many times have you heard of cases where Canadian damage insurance companies had violated an individual's privacy?

Mrs. Carole Lavallée: That information is not made public; the issue is handed over to the Privacy Commissioner of Canada, who, in turn decides whether or not to disclose the information publicly. To my knowledge, she has not made much information public in the three last years.

Mr. Mark Yakabuski: It is precisely because insurance companies fully understand that personal information is sacred and must be protected as such.

We are already subject to a good number of regulations. As Ms. Bercovici has already mentioned, all insurance companies are subject to the law of good will. It is a principle of common law which is absolutely sacred. It is in the contract between an individual and an insurance company. The Supreme Court of Canada has already noted that when a company violates the principle of good will, this may cost it millions of dollars.

The government's job is to legislate, but not to overlegislate. There is a gap when it comes to how work product information is regulated. Therefore, I am recommending that you legislate on this particular matter.

Where insurance companies and the protection of personal information is concerned, there are already many regulations in place, in addition to the Office of the Superintendent of Financial Institutions. Madam, one should avoid overlegislating.

[*English*]

The Vice-Chair (Mr. David Tilson): Thank you.

Time has expired, but we'll give you a couple of moments, Mr. Long.

Mr. Murray Long: Thank you very much.

You don't pass privacy laws to require good corporations to act responsibly. You pass laws because you have other companies that don't accept those responsibilities. The very first complaint investigation under the Alberta privacy commissioner's office involved three companies that had disposed of very detailed personal records containing tons of personal information, financial data, by putting those into the dumpster. The only way those companies were found out was when the Edmonton police force found the records, which were being sold to identity thieves, and it was able to go to the Privacy Commissioner and say they knew where those records came from.

You need to have a breach disclosure requirement that requires all companies to act responsibly. There is a great risk, even though insurance companies, I'm sure, will do the right thing. There are lots of other corporations and small businesses in Canada that might see the reputational effect going the other way. They would rather hide the fact that they had breached the law and not disclosed to anybody that their data had been stolen. So you could have your credit compromised, and unless the police did the investigation and found out the source, you might never know where the data breach had actually happened. I think there is a requirement to have some kind of disclosure mechanism built into the act and to have some kind of penalty there to encourage small businesses to actually obey the law.

The Vice-Chair (Mr. David Tilson): Thank you.

Mr. Dhaliwal.

Mr. Sukh Dhaliwal: My question is for Mr. Yakabuski. One interesting topic that he brought up is the garage information.

I certainly agree with you when it comes to insurance companies. I have never had an experience in the last 20 years where my personal information has been given out.

You mention the garage situation. There are big companies like GMC and Chrysler. These days they have equipment that diagnoses cars for any faults or issues. These small garages have come to me many times and they have brought up this issue with me that they don't have access to that technology. What would you call that? Would you call this a work-related issue or would you call this a company product issue to do with that situation?

● (1045)

Mr. Mark Yakabuski: I don't think it's a work product issue. I am familiar with the issue you're talking about. I can tell you that I actually had a meeting with the Automotive Industries Association of Canada last week to discuss how we can facilitate discussions among the vehicle manufacturers and the garage repair people across Canada so there is some degree of access to software codes they need in order to properly repair these cars. That is all part of the to and fro of a good vibrant economy. No one is going to give that information, if you will, with nothing in return. So it is an issue that requires discussion, and we will be there.

Mr. Sukh Dhaliwal: My question is back on this reasonable and minimal piece. There might be some instances where you feel there will be some individuals who might not be able to afford...or might not have the resources, as other businesses or individuals might have. How would you address that situation?

Mr. Randy Bundus: That's a difficult question. What you would be asking is for the business to subsidize the cost of making this access request. The problem we face by forcing the insurers or big businesses to respond at a minimal fee is that they can be subject to tactics. They can be oppressed, in a way, in the course of a court action, where the threat of a request for boxes and boxes of file material is made in the knowledge that it would cost huge amounts of money to respond. Even though the case may be one that the insurer or the defendant would like to have the courts resolve, it's more cost effective to pay the claim off than to respond to the PIPEDA request. So to avoid abuses by certain parties that may wish to use PIPEDA as a sword in their litigation process is largely the reason we are concerned about the responsibility to have to respond with minimum rather than the reasonable fees.

Mr. Sukh Dhaliwal: Is there someone else who wants to add something?

Ms. Ann MacKenzie: I want to comment on the issue of minimum fees for producing, and I agree with Mr. Bundus that there are times when the requests are abusive. There are times when if you ask for a minimal fee.... I want to comment on one thing. Let me rephrase this. The cost isn't just borne by the companies, it's borne by the people who buy the products. The more expensive you make the delivery of the system, the more expensive the product's going to be.

This issue doesn't happen every day, but when it does happen it is abusive. It's people who want to abuse the system by making repeated requests for thousands and thousands of documents just to slow things down.

So I think it is fair in certain cases to ask for minimum fees. We do it in the court system. If we were in court and were required to produce documents, we could do so at fees, and nobody has a problem coming up with something that's reasonable; there are standards for it. So I think it is something that already happens. It's just looked after by the process.

Mr. Sukh Dhaliwal: Mr. Long has something to add, Mr. Chair.

Mr. Murray Long: I have a concern that if you move to a sliding scale such as reasonable fees you can end up in a situation where they become deterrent fees, and people feel that they can't afford the cost of an access request and therefore they are denied access to the fundamental information to which they're entitled to have a right of access.

I think there are some other ways of resolving some of these kinds of concerns where people are making requests that are clearly made in bad faith or made in a vexatious manner. Under the B.C. act, the company is entitled to go to the B.C. commissioner and say we would like the right not to have to respond to this access request because we think it was made in bad faith, or is frivolous, or is vexatious. I think that's certainly one thing you may want to look at putting into the act.

Certainly, when you start sliding the scale towards “reasonable”, which is a hard term to really interpret here, if you get beyond the minimal or no fee approach—and I think there are schedules you can use to look at what actually is a minimal cost, the cost of photocopying things and so on—I don't think the individual should have to bear the burden of the corporation saying, we have to do some research to know what to give you. I think that should be the company's burden. I think to impose the burden back on the individual is patently unfair. The company has collected and is using their information for their economic benefit, usually, and the individual should not have to pay a new cost on top of that to have access to it.

● (1050)

The Vice-Chair (Mr. David Tilson): Thank you.

We're coming to the end of our time. The chair has one question of Mr. Long, and that has to do with the notification issue that you spoke of in your presentation. I don't recall anyone...I think you've gone a little further than most—

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

Mr. Murray Long: I think I have.

The Vice-Chair (Mr. David Tilson): If it's been suggested, I don't recall it. Your suggestion is that if the notification isn't complied with, whatever notification it is, there would be a penalty. I find that interesting. Have you put your mind to who would have jurisdiction over that? Is it the courts, the Privacy Commissioner? That's the first question.

The second question is, have you thought of a minimum penalty? We don't have much time, but the third question would be, would this requirement apply to foreign companies—which I'm sure will get the insurance industry all excited—that have subsidiaries here in this country?

Mr. Murray Long: If there are subsidiaries here in this country, they're subject to our law to the extent they are collecting and using information inside Canada. I think that's fairly clearly understood.

With regard to the offence, section 28 of the act already outlines what the offences are at the present time. There are certainly offences for obstructing the Privacy Commissioner in performing her duties. Those fines range from $10,000 to $100,000. Generally speaking, it would be through the Attorney General, and there'd be some kind of a hearing or trial, whatever, to establish the fine. It would be an offence under the act, though.

In the case of breach disclosure, any organization that knowingly withheld information about a breach, knowing that it could cause public harm or loss of, say, credit standing, cause the kind of harm that we associate with identity theft, if they did so knowingly and without regard to the public interest, I think that should be considered a serious offence under the act. I think there needs to be some kind of a penalty put in place in the act to make especially smaller companies that may not have the kind of fiduciary responsibilities or sense of obligation that large corporations have understand that this is a serious issue and it will be treated as a serious issue.

Mrs. Vivian Bercovici: May I interject, Mr. Chairman?

The Vice-Chair (Mr. David Tilson): Yes, Ms. Bercovici.

Mrs. Vivian Bercovici: I'd like to take you to tab 4 of our materials, which was the transcript, so there's a little déjà vu here. It's at tab 4, page 4, in both the English and French versions, towards the bottom of the page. We don't disagree—which is a roundabout way of saying we pretty much agree—that there should be a duty to notify. The problem isn't whether there should be a duty to notify, or whether people have the right. The problem is the threshold. When you're dealing with a principle-based statute with the breadth of PIPEDA, it's almost impossible to craft a meaningful threshold. This is something—if you look at the bottom of column two—which the commissioner acknowledges quite explicitly. She says, "we're in favour of the principle. The problem is in knowing how to implement it." She continues on to talk about the complexity and the difficulty in trying to transpose the American remedies to Canada. "To whom do you give notice? What would be the scope of it? Would it concern all the information, or only where there's significant risk? Who will bear the cost?" If you turn over to page 5, midway down, she says that she recommends there be a breach notification provision. The exact wording, however, is quite honestly a challenge, and then there's a discussion about needing some sort of threshold.

With respect, we would suggest that you consider that perhaps there be some sort of statement of principle in PIPEDA, that there should be notification with some sort of threshold, but then again, we would suggest, particularly with complex industries like ours, that the detail of exactly what the threshold is going to be and how it's going to be implemented be left to our governing statutes and to those who really have expert knowledge of how we function. You can put rules. It's very difficult to put in rules that are going to apply to banks and to a small business. There's another passage in here where we have the commissioner and assistant commissioner talking about the CIBC breaches. You can have rules upon rules, but sometimes things are going to happen. They said CIBC did everything right. They had great systems. They had great agreements, but sometimes these things happen.

I would suggest—and we would I think agree on this—that it be left to those with expert knowledge of our very complex industries.

● (1055)

The Vice-Chair (Mr. David Tilson): I appreciate that interjection. We've run out of time. You've raised many issues for the committee to consider, and I thank you for bringing your knowledge to us.

Thank you very much.

This 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
