House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 031 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Thursday, February 15, 2007

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 15, 2007

● (0900)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): Good morning. This is meeting 31. Can you believe that?

We're still working on the PIPEDA review. Today we have the Canadian Federation of Independent Business and the Consumers' Association of Canada. From the CFIB we have Corinne Pohlmann, director; and Lucie Charron, policy analyst. With the Consumers' Association we have Margaret Anne Ireland, director. Bruce Cran would have liked to be here but he's in Vancouver, snowed in, which is almost an oxymoron, but there you go.

Welcome to you all. You'll have up to approximately 10 minutes to make your opening comments. Then we'll go to questions from the members.

We'll start with Ms. Pohlmann.

Ms. Corinne Pohlmann (Director, National Affairs, Canadian Federation of Independent Business): Good morning. As mentioned, my name is Corinne Pohlmann. I am the director of national affairs for the Canadian Federation of Independent Business. With me today is our policy analyst, Lucie Charron, who will be supporting me through the question and answer period.

I have been in this position for about a year, and for the six years prior to that I was in Alberta as CFIB's director of provincial affairs. In my experience there I was involved in the implementation of the Personal Information Protection Act and saw its impacts on Alberta's small and medium-sized companies. In fact, until my departure about a year ago, I was a member of the ministerial advisory committee on Alberta's privacy act, providing feedback on how well SMEs were adapting to the legislation in that province.

First I'd like to share just a little bit about CFIB. We're a non-partisan, not-for-profit organization that's 100% funded by our 108,000 members, who are independently owned and operated small and medium-sized businesses from across the country. Our members come from all sectors of the economy, and they're found in all regions of the country.

You should have in front of you a slide deck. The first slide shows the profile of our members. You'll notice that our membership is a pretty good reflection of the general business population, which as you know is dominated by small and medium-sized companies.

The chart at the top of the next page illustrates the fact that more than 97% of Canadian businesses have fewer than 50 employees. These businesses represent approximately 45% of Canada's GDP and employ almost 60% of all Canadians. They also continue to create the bulk of new jobs in our economy.

As you can see on the next chart on that page, using Industry Canada findings, of the almost one million jobs that were created between 1993 and 2003, close to 80% were created by small firms, which they define as those with fewer than 100 employees.

Why do I show these to you? It's to emphasize the growing importance of SMEs and to encourage you to always think about how government decisions can impact this integral part of Canada's economy. What may seem trivial to a larger firm can be of great significance to a smaller firm. It can add more cost, confusion, and paperwork, thereby adding more stress for the average small business owner.

So what is top of mind for SMEs? The chart on the next page shows you the issues of highest priority for our members, which we collect on an ongoing basis, face-to-face, through a survey process. We then aggregate those results every six months. This information provides us with direction on which issues we need to take on as an organization.

I'd like to highlight the second highest issue of concern for Canada's SMEs: government regulations and paper burden. This really comes as no surprise when you realize that the cost of regulations tends to be much higher for smaller firms. As you'll notice in the smaller chart, this is illustrated quite well using both CFIB and OECD data. It has been supported by data out of Quebec and the United States that the smaller the firm, the higher the cost per employee to deal with regulations.

That is why we have been so pleased to see commitments being made by provincial governments such as British Columbia, Quebec, and Newfoundland and Labrador to tackle this issue and commit to measuring and reducing the regulatory and paperwork burden on business. More recently we were very pleased to see the federal government also make a commitment to a 20% reduction in the paperwork burden on business.

This leads me to the issue of PIPEDA. Our members in all provinces and territories without their own provincial law are expected to comply with PIPEDA when it comes to dealing with public and consumer information. You should know that we are not legal experts on the technical aspects of the law. Rather, we are here to provide you with some feedback on what we have learned about how SMEs have dealt with this legislation.

First, our members are consumers as well as business owners, so they're concerned about making sure their own personal information is protected. As a result, they are also conscious of protecting the privacy of their clients, customers, and employees.

As far back as 1996, we asked our members about the need for the federal government to introduce a national privacy legislation. Based on more than 10,000 responses, you will see on the top slide on the last page that our members supported the notion of a national law protecting personal information right across Canada. As a result of this finding, CFIB has never argued against the national law. In fact, we believe that for this law to be truly effective it must be adopted by SMEs across Canada. In order for that to happen, it cannot be complicated or onerous to comply with. So the focus of our work has been to ensure that the legislation is simple to understand and does not impose a significant burden on small businesses.

● (0905)

We do actually view PIPEDA as workable legislation from a small business perspective because it avoids prescriptive solutions and allows for flexibility in how businesses can respond to its requirements. The act understands that not every business manages huge amounts of personal information, and that the types of information can vary substantially from sector to sector, and from business to business.

We also like the balance it achieves between protecting consumers' interests while understanding that businesses need information to provide products and services. As mentioned, our members support national privacy legislation—after all, they are consumers too—but they're also business owners who may sometimes need to ask for personal information to be able to offer the public or its employees what they demand.

We also support the fact that it is a complaints-driven process. Regulations and paper burden can be stressful for small business owners, who tend to wear several hats in their business, from human resources to sales to marketing—you name it. It's usually the owner who's responsible for protecting personal information as well. We do believe that most are already doing what they can to protect personal information in their possession as a matter of good business practice. They may simply have not yet put it down on paper and formalized it.

Keeping the process complaints driven removes the level of stress for the SME owner who may otherwise fear being inspected or even fined if they've not complied to the exact letter of the law.

We also believe the ombudsman model works well. It is less intimidating for a small business owner to approach the commissioner's office to ask questions about their own privacy compliance issues.

Since its implementation on the broader private sector three years ago, CFIB has handled hundreds of calls from small business members across the country looking for direction on how to comply. To handle the questions, we've created a dedicated page on our website with links to where they can get more information. We've put together a handout summarizing their obligations, of which you have a sample in front of you. We also offer our members an online course for free on how to manage private information under PIPEDA.

While most calls came during the first phases of implementation in 2004, we continue to get inquiries on a regular basis. By far the most common calls we receive are questions on how to comply—specifically, how to put together a privacy policy for customers and for employees, and whether or not a template is available for them to use. We know a template was developed in Alberta and British Columbia specifically for SMEs, so we've been encouraging and we will continue to encourage the commissioner to consider producing something similar for PIPEDA.

Finally, you may be curious to know how well SMEs are complying with PIPEDA. While we do not have specific information for PIPEDA, we do have...members in Alberta who were asked this question in relation to the provincial legislation introduced at the same time.

On the last page you'll find a table of our findings, which were that most business members in that province, between 70% and 80%, were aware of the legislation, but far fewer had developed a formal privacy policy. The good news is that compliance is increasing, with 40% saying that they had a formal written policy in 2006, which is substantially higher than the 31% who said they had such a policy in 2005.

So what does all this mean? Well, at this point we do not see any need for substantial change to the act and request that PIPEDA be given more time so that SMEs can gain more experience with the law in its current form. Making changes at this early juncture could needlessly complicate the process and make it even more difficult for SMEs to comply. In other words, we believe more time is needed to really understand the full effect of this law on SMEs and consumers.

In the meantime, CFIB will continue to do what it can to help our members and the general small business population understand their obligations under the law.

Thank you.

● (0910)

The Chair: Thank you, Ms. Pohlmann.

Before we go to Madam Ireland, you referenced a piece of paper—I think I'm holding it in my hand—"Privacy Legislation". I'm just curious to see it's very dated. Is this your most recent handout for your members? It's talking about the act coming into force.

Ms. Corinne Pohlmann: Yes, it is the most recent, but we actually have a website we refer our members to that has more up-to-date information. We also refer them to the online course, which has also been updated.

The Chair: Thank you.

Ms. Ireland, please.

Ms. Margaret Anne Ireland (Director, Consumers' Association of Canada): Before I begin, I have to offer Mr. Cran's regrets. He was a victim of our snowstorm yesterday and was unable to get out of Vancouver.

My name is Margaret Ireland. I'm a member of the board of directors of the Consumers' Association of Canada.

We would like to thank you for inviting us to speak to your committee this morning.

The Consumers' Association of Canada is a 60-year-old, independent, not-for-profit, volunteer-based organization with a national office here in Ottawa and with provincial-territorial representatives. Our mandate is to inform and educate consumers on marketplace issues and to advocate for consumers with government and industry, and to work with government and industry to solve marketplace problems in beneficial ways.

At the time PIPEDA was enacted, we were only beginning to see the various ways that personal information could be mishandled or misused. Sufficient time has now passed to show us which types of improvements need to be made to the act. It's become quite obvious that theft of personal information from corporate data banks, specifically, is out of control. Voluntary guidelines have proven worse than useless, and the time has come to put some strict protection in place for Canadians, with some serious consequences for those who place consumers at risk. We believe the Office of the Privacy Commissioner should be given some real teeth. Regulations and penalties that are meaningful and rigorously implemented could make an enormous difference in the everyday lives of Canadian consumers.

It is time to move from voluntary guidelines for the protection of personal information to actual regulation designed to ensure that those entities collecting information have clear rules about what information they can ask for, what they can do with it, how long they can keep it, and what measures they must take to protect this information. This, together with stiff penalties for breaching these regulations and rules on notification of citizens when their information is compromised, will help reduce the disastrous consequences of identity theft.

Limiting the type of collectable information to the bare necessities is the first step. We have specific concerns about what type of information is collected from consumers and how this information is handled. We would also like to see limits on the length of time that corporations can keep this information and restrictions on sending it outside the country. There is very little reason for a company to keep, for example, a consumer's credit or debit card number in their computer system for extended periods of time unless they have an ongoing relationship that requires this.

In addition, we would like to be assured that the process, which is now ongoing, where all automated debit and credit card transaction records are obscured, is completed by the end of the year. We oppose sending Canadians' personal information, either financial or health information, outside this country. Removing this data from Canadian jurisdiction puts each of us at unnecessary risk, with no actual benefit to consumers.

In conclusion, I will be absolutely blunt. We do not believe that some commercial enterprises' right to collect a consumer's personal data for marketing purposes can be allowed to outweigh the rights of the consumer to be safe and secure in this day and age of international computer hacking, fraud, and identify theft. The only way to ensure that data are not hacked is not to have them available in the first place.

Thank you.

● (0915)

The Chair: All right, a very direct presentation. Thank you very much.

I detect a little disagreement among the panellists, so this should provoke some interesting questioning.

Our first round is for seven minutes, and we'll start with Mr. Dhaliwal.

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

Thank you, panel, for coming out.

My first question is to Ms. Pohlmann. In your presentation you show that most of the businesses in Canada are small businesses. Could you tell me what challenges these small businesses are facing, in your opinion, when it comes to PIPEDA?

Ms. Corinne Pohlmann: When it comes to PIPEDA, I think the biggest challenge they're facing is understanding what their obligations are. Most small businesses in Canada are not going to be handling huge amounts of personal information. Many of them don't necessarily always deal directly with the public, and so I think it gets a little complicated to understand what it is they need to do to comply.

The biggest question we always get is that they want to comply but they don't understand what they need to do. The irony is that most of them are probably doing it already. It just hasn't been formalized on a piece of paper, and that's the big challenge they face. So having some sort of tool that can help them understand how to put it down on that piece of paper to say, this is what you need to do to make sure you're protecting the public's information and your employee information.... Many of them are also calling on that, even though under PIPEDA most of them are not required to do so. I would say that's probably the biggest challenge they face.

Mr. Sukh Dhaliwal: You say they do not know how to protect the information. Are you aware of any breaches in small businesses that are offering a reference to PIPEDA?

Ms. Corinne Pohlmann: No, we're not aware of any breaches. I would suggest that if a breach did occur, it would likely be because they weren't aware of what they were supposed to be doing in the first place to make sure. But I am not aware of any serious breaches at a small business.

Mr. Sukh Dhaliwal: I was going through this pamphlet that you have. You say what personal information is, and it's quite a big definition. In particular, we heard from witnesses earlier that we should distinguish between personal information and work-related information. When I look here, you say medical records, ID numbers, and loan records, and the list goes on. From your understanding, where would you say we should be able to draw a line between personal information and a work product?

Ms. Corinne Pohlmann: That's a difficult question for me to answer. I don't have a legal or technical background in that respect. A lot of small business owners looking at how to protect personal information would probably think about it from the perspective of what they would want protected if it were their own information. I think that is how they would probably look at what they would decide to protect and what could probably not be protected as much. I think medical records and loan records and so forth need to be protected.

The other thing is that we had to build it so that it was national in scope; we had to make sure that it also underlined the fact that in some provinces there are medical information laws they have to comply with, and in other ones there aren't. We tried to make it a little more holistic in that respect as well—that it wasn't just PIPEDA, and there were responsibilities under other laws that might also implicate them with some provinces.

Mr. Sukh Dhaliwal: Do you see that we should have a clear definition of the work product, or do you think we should leave it to the small businesses to interpret on a case-by-case situation?

Ms. Corinne Pohlmann: It think it would probably be best to keep it to a case-by-case situation. Defining a work product—I'm not 100% sure exactly what that means, to be honest with you, and I'm not so sure a business owner would know what it means. I think that would be part of the issue. Perhaps defining it a little bit better is not a bad thing to do, so that they can be more clear on the differentiation, but it gets complicated, because when you're a federally regulated company or a company in Alberta or B.C., you're dealing with different rules again.

● (0920)

Mr. Sukh Dhaliwal: Mr. Chair, would Ms. Ireland have anything to add?

Ms. Margaret Anne Ireland: Regarding the employee relationship and so on, we don't delve into that area. Our sole focus is consumers; we have a focus on the types of issues that affect consumers directly in their personal and private information.

Mr. Sukh Dhaliwal: Even if you're working for the consumers, do you see a need for personal information and work-related information in those small businesses? When we talk about small businesses and medical records, all the physicians are small businesses. They fall under that category. That's where I was coming from.

Where do you see, from a consumer perspective, that we should be able to draw a line? For example, a person goes to a doctor. As long as they don't disclose their name, their date of birth, their ethnicity, or what not, and as long as they're able to disclose what kind of medicine they get or what kind of disease they have or what kind of treatment they get and what not, would you call that personal information or would you call it work-related information?

Ms. Margaret Anne Ireland: I think I see what you're getting at. The health field in particular is a little different, because many people probably do disclose more information in that area than in any other aspect of their lives.

To a large extent I have enough faith in my own doctor that I still have a good view of the medical system. I have been comfortable personally with disclosing a fair amount of information, even though it may become part of his work product. I am relying on their ability to keep it confidential.

To this point we haven't seen a great number of difficulties with consumer information being breached in a medical situation. It hasn't been a huge issue related to the type of thing you see when a data bank is hacked and everybody's credit card numbers are stolen, or something like that; it seems to be a difficult type of scale.

Mr. Sukh Dhaliwal: Where do you see that personal information is breached, if it's not medical? Is there a particular field in which this breach—

Ms. Margaret Anne Ireland: Our only concern was the one specific instance in which medical information was sent out of the country from British Columbia. It was not properly handled.

Mr. Sukh Dhaliwal: And ended up in the garbage bins and on the streets.

Ms. Margaret Anne Ireland: Yes, and that is part of the reason we object to having personal information sent out of the country. As long as it is held within the country, it's subject to PIPEDA and other regulations, and we feel it's much easier to control the access.

Mr. Sukh Dhaliwal: Thank you.

[*Translation*]

The Chair: Mr. Vincent for seven minutes.

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

My question is for Ms. Pohlmann. Mention was made earlier of business products. I see that you mention personal information such as age, weight, marital status, disciplinary measures and credit history.

In your opinion, could personal information of the nature stated in your document be considered a business product?

Do you not have that document?

Ms. Corinne Pohlmann: I don't. I had turned everything over to the clerk. I'm sorry.

● (0925)

Mr. Robert Vincent: I understand. However, what do you consider to be a business product?

Ms. Corinne Pohlmann: To my mind, a business product is primarily a person's work address, the employee's e-mail address that is given to the employer. This is information that the company has about the employee, details that are part of his work.

Most SMEs do not use a great deal of information. Occasionally, retailers use information about credit cards, but systems already have ways of protecting this information.

I'm not very familiar with work-related information. I'm not clear as to what details are important in terms of the regulations.

Mr. Robert Vincent: You mentioned retailers. That surprises me, because according to a fact-finding report released in 2006, out of a total of 64 retailers working via the Internet, virtually none was aware of the requirements under the act.

Would you care to venture an opinion on the subject? You said that you had given a short course. What did this involve in terms of training members of your association?

Ms. Corinne Pohlmann: I would be easier for me to answer that question in English.

[*English*]

The course itself is really just an overview of PIPEDA and what their responsibilities are under PIPEDA. So it would essentially take the rules and regulations under PIPEDA, what they need to do to build a template, and what they need to understand in order to protect their clients' information.

It doesn't really get into much more detail than that. It's meant to be a way for them to get an introduction to privacy information and what they need to do to protect it. It's also meant to give them an idea of whether they're holding information that's considered very personal, versus what's not as personal. Also if they have personal information of a more important stature, then perhaps they need to get some help on how to protect it.

So we're not telling them how to do this. We're basically showing them the guidelines and what they need to do to take the next steps.

[*Translation*]

Mr. Robert Vincent: When these people want to destroy personal information that has been in their possession for several years, do they proceed in any particular way? Do the companies with whom you are involved have a specific way of destroying these documents, or do they simply throw them out with the trash, or some such thing? Are special steps taken to destroy this type of document?

Businesses also trade lists of members or employees as well as personal information. Are you aware of any businesses that do this?

[*English*]

Ms. Corinne Pohlmann: Within our own organization?

[*Translation*]

Mr. Robert Vincent: Yes.

[*English*]

Ms. Corinne Pohlmann: Yes. Our organization has a privacy policy. It's on our website. When we no longer need business information in records and data bases, it is destroyed.

We give our policy to our members who ask how to build a privacy policy. This is the type of information we collect as an organization and this is what we do to protect information. We use it as an example for our members.

[*Translation*]

Mr. Robert Vincent: How do you go about destroying these documents?

[*English*]

Ms. Corinne Pohlmann: It would be shredding the files. If anything is in the database, it would basically be cleared and destroyed.

[*Translation*]

Mr. Robert Vincent: I see, because we've seen where people have placed documents like this in boxes that have then been thrown in trash bins. It is quite common for small businesses not to give much thought to protecting people's personal information.

You're not aware of similar things happening? You know what happens in your organization, but you're not aware of what other members of your association might be doing.

Do you have any recommendations to make to us today concerning the protection of personal information?

● (0930)

[*English*]

Ms. Corinne Pohlmann: We believe the current regulation, as it exists, hasn't had the time to really be implemented. We would like to see it fully take effect so that SMEs are complying with it 100%. I think it has taken some time to get off the ground.

I believe SMEs don't like prescriptive regulations, because generally speaking it's difficult for them to comply. The more restrictive a rule becomes, the more difficult it is to get them to comply. Giving a principle approach allows them to decide for themselves the best way to deal with consumer information.

I'd like to remind you once more that our members are also consumers. They believe it's important to have national privacy legislation. They will try to do the best they can to protect that information. I think the approach you're taking now is a more effective approach in helping them comply with protecting personal information. Trying to be more restrictive will just cause more confusion and fear.

The Chair: We'll go to Mr. Tilson, followed by round two, beginning with Mr. Pearson.

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

I'd like to ask a question. It has been suggested by some witnesses that there should be an amendment that would require you to notify your public of a breach. Either last year or the year before, a whole bunch of information was found in some scrap yard in the southern states. Then we had the Winners situation a number of weeks ago. CIBC lost the data of 470,000 people, which included client names, addresses, signatures, dates of birth, bank account numbers, beneficiary information, and/or social insurance numbers.

A story came out this morning on the news. I don't know what's in the press, but it was on the television. It said that CIBC—I think it was CIBC, one of the banks—was sending out new credit cards to everyone, but they weren't saying why. Why was that? Was that as a result of the loss of all this information?

I understand business. Whether it be the big banks or individual businesses, the cost of notification would be unbelievable. On the one side, I understand that dilemma. On the other side of the coin, people want to know. They want to know whether someone has their social insurance number, or their names even.

Could both sets of witnesses comment on that? My specific question is whether notification of a breach should be a requirement.

Ms. Margaret Anne Ireland: Actually, I believe the incident you're referring to involves the Bank of Montreal. We've been receiving phone calls over the last few days. For instance, some people got a letter, were told to phone, and weren't able to get through on the phone. Some showed up someplace to use their credit card and were told the credit card was no longer valid. Or because so many people had received cards in the mail, when they tried to phone in to activate their cards, the lines were busy.

So we've received a number of phone calls over the last few days about this. It is something we're very concerned about. It's very difficult for consumers now to keep track of who has what information and where it might be.

If a security breach happens and someone gets your credit card number or your social security number, you may not know for months and months. By then untold damage can be done. In the case of identity theft, you're looking at a destroyed credit rating or an inability to get a mortgage. In some cases, a credit rating can affect employment, because some employers do check your credit rating before they hire you.

● (0935)

Mr. David Tilson: Should the bill be amended to make it mandatory for customers or the public to be notified of any form of breach, whether it be—

Ms. Margaret Anne Ireland: Absolutely.

Mr. David Tilson: The banks, or I think at least the banking people—I hope I'm not misquoting people—have come across and said, you know, if there's a suggestion of fraud, we'll notify.

Now, that's a pretty vague statement, but that's what they've said.

Ms. Margaret Anne Ireland: We absolutely believe that notification should be mandatory. It would be nice if they would also explain to these people why they're changing their credit cards. No one has been told why; it has just been, here you go, you're getting a new card. And of course this raises all kinds of suspicion in people's minds, which is part of the reason we're getting the phone calls.

Speaking personally, two years ago the Bank of Montreal did the same thing to me. They phoned and told me they were sending me a new card, and not to use the one I had. When I asked why, they said they couldn't tell me. Even when I said again that I wanted to know, they said they couldn't tell me.

Mr. David Tilson: Okay. I want to hear what the CFIB thinks about this.

Ms. Corinne Pohlmann: I do believe that actually having people report when there is a breach is important when there's a risk associated with the information that's been breached. I think businesses should be required to let their customers know if there has been a major breach in terms of the information that has gone out—for instance, if it includes credit card information, SIN numbers, medical records, all those types of thing. But I would think that there are probably different levels of breaches, and I would suspect that sometimes a breach can be fairly minor, and won't have a huge impact on the public.

The other side of this, and one where I can see the business community and I think our members having some concerns, is the fact that they may not even be aware of why the breach occurred. It could have been something that was stolen from them, for instance, or wasn't really their fault.

Those are the situations where it becomes difficult and where perhaps there is a responsibility, I believe, to notify those that have been affected by it. At the same time—

Mr. David Tilson: Should there be an amendment to the legislation?

Ms. Corinne Pohlmann: I think it would depend on the level of breach. If it's a breach where there's a risk to the consumer, then yes, I think they should be required to report—

Mr. David Tilson: And what if they don't? Any ideas?

Siberia, someone says.

Do I still have time, Mr. Chairman?

The Chair: You have one minute, but Ms. Ireland may want to say something. In her opening remarks, she said there should be meaningful penalties.

Ms. Margaret Anne Ireland: We would like to see significant penalties in the case of a major breach. I'm thinking in terms of something like the Winners incident. I would go as high as saying that they must notify each individual customer, with penalties up to $100,000, escalating for each incident. Make it serious.

Mr. David Tilson: And the independent business federation?

Ms. Corinne Pohlmann: It would depend on how the breach occurred. I do believe that sometimes businesses are not aware of it, or may not have been the cause of it.

Imposing a $100,000 penalty on a small business—versus a large bank—would put them out of business. When you talk about levels of breaches, and the impacts on the business community, I think you have to be very careful when you start going down that road.

The Chair: Thank you, Mr. Tilson.

This is a five-minute round, Mr. Pearson.

Mr. Glen Pearson (London North Centre, Lib.): Good morning, everyone.

My question relates to something in your presentation. In the business area, you asked whether the federal government should introduce national privacy legislation, and you have Alberta with 52% saying yes.

In the area below, you have the awareness of the need to protect personal information in Alberta. In 2005 it was 80%, and in 2006 it's 70%. It seems to me to be going the wrong way. Could you explain why that is, because we have heard often about the Alberta model. I'd just like to know that.

Ms. Corinne Pohlmann: Yes. Part of it is that the question slightly changed. The question in 2005 was whether they were aware of their obligation to protect personal information. In 2006 it was whether they were aware of the Personal Information Protection Act, PIPA.

So I think the first instance is really that they know they have protected information. They may not know that there's an act related to it. I would suggest to you that it probably continues to be around the 80% mark in Alberta. So it's the slight difference in the wording of the question that we believe caused that blip-down.

Mr. Glen Pearson: All right, thank you.

When chambers of commerce were in here and we discussed with them earlier, they had done a lot on their website to make members aware of what was required under PIPEDA. I asked them what was happening in return, how they got the information in return from businesses as to how they felt about this. Do you know what I mean? It's not just your trying to provide direction and make people aware. Have they found it too onerous? What kind of mechanisms have you set up so that they can return information to you on how they feel about this?

● (0940)

Ms. Corinne Pohlmann: We're a heavily survey-based organization. Really the only place we've surveyed is Alberta, but our other avenue is that we have counsellors across the country who deal with member inquiries on a daily basis. We have had probably thousands of calls over the course of the last three years from small businesses on this issue. I did go through a lot of those logs in preparation for this, and I would say, as I mentioned in my opening remarks, that the bulk of the calls came in 2004, with its implementation, when people were trying to understand what they had to do.

We continue to get calls, though, on a fairly regular basis. Now I would say 90% of those calls are about compliance and about how to write a privacy policy, essentially. They just want to understand what they need to do to put it down on paper and to make sure they're compliant with the law.

This is why I hesitate to put in prescriptive information, because then instead of thinking about what they need to do to really protect personal information—which is what the principle approach, I think, does—they'll just make sure that the privacy policy adheres to the specific rules that are put into the legislation and not necessarily think what they can do best in their firm. The principle approach allows them to think about how they can best deal with the information, and so we try to guide them through that process. When it becomes clear to us they have lots of personal information to protect, we suggest they see a consultant to help them put it together.

Mr. Glen Pearson: My final question is this. Mr. Dhaliwal asked you a question, and you responded to him by saying that you would prefer to see it handled on a case-by-case basis. We've had witnesses come before us and say that deciding everything on a case-by-case basis provides real uncertainty for future planning and other things. Can you make a comment on that?

Ms. Corinne Pohlmann: I think it relates back to the fact that privacy policy is going to be different for every firm because every firm has a different amount of information that it's protecting. So to expect one size to fit all in this particular scenario, I think, is incorrect.

Our fear is that the bar is always put at the highest. So you create rules that'll fit the banks, but they ain't going to be fitting the small businesses. The flexibility of this particular legislation is what we like about it—the fact that it's a principle approach and it allows businesses to do what they think is best to reach the end goal, which is to protect personal information. We would like to see that continue going forward, because once it becomes more prescriptive, we fear that our members will be lost when it comes to doing it correctly.

Mr. Glen Pearson: Some of the contention we've seen at this committee is that small businesses would rather have it that way. Larger ones would rather have it—

Ms. Corinne Pohlmann: Be more prescriptive.

Mr. Glen Pearson: Yes, that's right.

Thank you, Mr. Chair.

The Chair: Thank you.

Mr. Van Kesteren, *suivi par M. Ouellet.*

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you all for coming. I'm so glad to see you. I've been a member of your organization since 1987 and still am. I can testify that you do a great service to small businesses.

I have to say that when I read what the act covers, it conjures up images of exactly what you talked about when I was running my dealership. We saw this sort of stuff. We said, oh gee, it's exactly like you said; that's all we need.

I'm looking at accountability, the access. We must appoint an internal privacy expert commissioner with knowledge. You're absolutely right, a small business is totally hampered by those things.

As we begin to examine this whole privacy commissioner issue, there appears to be—and I want you to make a comment on this—a dividing line. I'm speaking to the consumers as well. Many of the problems, and much of the seriousness of privacy, seem to concern the larger firms more. When I look at your chart and see the incredible numbers—and I am familiar with those numbers, but every time I see them again, I am astounded by them—that this is the engine of our country....

Am I right in assuming this, or can you make a comment? Is this something that has more to do with larger businesses, larger corporations, that would possibly abuse it? Is there the same danger for a small or medium-sized business?

Could both sides make a quick comment? Ms. Ireland, could you please comment as well?

Ms. Corinne Pohlmann: My initial reaction is simply that a lot of small businesses know their customers personally. I think that makes a huge difference in terms of making sure they are protecting the people they know. This is their livelihood.

As you grow as a company, you may lose a bit of that. Therefore systems have to be put into place, and those sorts of potentials for abuse can happen. I think that's a big part of why you don't see breaches among smaller firms, because they're more aware of making sure they are protecting the people they know and rely on.

● (0945)

Mr. Dave Van Kesteren: Ms. Ireland, are you as worried about small businesses as you are about larger ones? Am I right on this?

Ms. Margaret Anne Ireland: We agree with the general direction you're going in here. Usually the smaller businesses don't collect as much information. They don't have it as accessible to a computer hacker. Frequently they do know their customers.

As far as privacy breaches of small businesses are concerned, what we tend to see is one person's information being inadvertently let out in an inappropriate way, as opposed to some kind of massive thing, where credit cards are going all over the place, and so on.

So definitely small business is different. We are not seeing the same kinds of problems.

Mr. Dave Van Kesteren: Obviously we're getting different testimony. There are two sides to this argument. There are those who say we should leave it the way it is. I'm wondering, can we make some adjustments that would allow consumers to feel a bit more comfortable, so that smaller businesses, the very engine of our industry, won't be hampered by that, and subsequently we won't suffer? As Bruce said a minute ago, all the things we ask business get passed down to the consumers, and so it results in higher costs.

Ms. Margaret Anne Ireland: We have not done any kind of survey, but what we are finding from the phone calls we receive is that very few consumers know anything about the act—that there is an act, that they can complain, and that there is an ombudsman they can go to. They have no idea, and this is an issue.

It's possible that if things were more widely known.... As the member over here said, surveys have suggested that many small businesses don't realize how the act applies to them or that there is an act, especially very tiny mom-and-pop outfits. This is an issue, and it's possible that more education may help toward solving this.

The Chair: I don't know if it's a help or a hindrance, but I don't know how many legislators are fully aware of the impact of this legislation. I was around when we passed this, and boy, have I learned a lot about the implications of what we passed since I've been on this committee. So we're all in the same boat in trying to protect consumers, while at the same time recognizing there are so many problems.

Monsieur Ouellet, followed by Mr. Stanton.

[*Translation*]

Mr. Christian Ouellet (Brome—Missisquoi): Thank you.

Ms. Pohlmann, my question is directed to you because, if I understand correctly, you maintain that all of your information is based on a code of ethics, more or less. You say that people, particularly those working in small firms, pay attention to what they're doing.

On looking at your table, we see that 56 of the businesses that belong to your federation are one-person operations with no employees. That's a fairly large number. This means that they do not necessarily have help destroying their documents. It also means that they may dispose of these documents in bulk.

Even if we assume that small firms face a lower risk than large firms because many people can be affected by errors that occur in large firms, the fact remains that in small businesses — and I know something about this area — information is often passed on from one person to another.

Do you have some way of preventing information from getting passed along from person to person within small businesses? What happens is that people know and call one another, requesting information about a particular individual. Ultimately, information ends up in the hands of someone other than the person requesting it.

How would your code of ethics and the voluntary compliance measures you mention limit this transfer of information?

● (0950)

[*English*]

Ms. Corinne Pohlmann: I don't think I talked about a code of ethics in terms of—

[*Translation*]

Mr. Christian Ouellet: No, I'm the one who said it. The fact that it is a code of ethics is what makes it voluntary.

Ms. Corinne Pohlmann: Yes, but this is based on our recommendations to members of our federation. However, in the case of small firms...

[*English*]

I don't think you can stop that. I don't know how you could, and I think it's a challenge for this committee to balance the fact that people want their information protected, but they want the convenience as well. They want to be able to buy online. They want to be able to set up their own little business or be a one-person operation and then find the clients they need by telephoning them. I think that's a challenge this committee faces in terms of trying to balance that protection with convenience and what people demand as consumers.

As for stalling an individual who is building a business and saying, you can't call that person and give them information, one, I don't know how you would police that, and two, that's how businesses are born. That's how they grow. That's how they make connections and network, and if you try to define that as work product information, I think that's difficult to do as well.

I don't know if I'm answering your question the way you were seeking, but I think it would be difficult to try to stop that, and I think it would also stifle entrepreneurship to a certain degree if you did try to.

[*Translation*]

Mr. Christian Ouellet: Thank you.

Ms. Ireland, do you share this view of the problem associated with controlling information within small businesses? That's my first question.

Secondly, you said earlier that we need legislation that would sanction violators and even impose substantial fines on them. In your opinion, how could the act be amended to provide some way of identifying flaws in the system? Putting it another way, aside from the cases reported on in the newspapers, how do we unmask companies that fail to destroy information after a certain number of months? How do we do that?

[*English*]

Ms. Margaret Anne Ireland: To answer the second question first, how can we ensure that anybody respects any law? We put them out there, we encourage compliance, and we do the best we can. That's always an ongoing issue with any of these types of things. It's always an educational process. Sometimes you teach people, and sometimes you have to push them in the right direction.

Frequently I have a fairly benign view of humanity. I believe most people are not bad. If you show them what it is and why it needs to be done, they do it. But there are also people who, for whatever reason, take a rather laissez-faire approach to some things, and they're probably the ones who need to get slapped.

I'm trying to remember the first question.

[*Translation*]

Mr. Christian Ouellet: I asked you if there was any danger of information circulating from one small business to another, without ever coming back to its source. We know that small business owners with no employees have little time to check back in their records. Isn't that right?

I once worked alone in a small firm and I know that the business always looked to the future and never went back and dealt with old files. That's not unusual in this case. People are there to work and to earn money, not merely to occupy a desk. Otherwise their business will fail. They are one-person operations, as we are seeing with 56% of the cases here.

So then, how can we ask them? Can we expect that after a certain period of time, they will dispose of the information in their possession?

● (0955)

[*English*]

The Chair: I'll ask the witnesses if they have any comments on that question, and then we'll move to Mr. Stanton.

Ms. Margaret Anne Ireland: Just quickly, I think that relates to one of our suggestions that the amount of information you can collect should be limited and the amount of time it can be kept should be severely restricted. If you're only keeping it for a very short period of time, if you're destroying it every month or every ninety days, then that's not an issue.

The Chair: Any comment, Madam Pohlmann?

Ms. Corinne Pohlmann: I'll just repeat what I said. Small businesses know their customers, they know their clients. They do the best they can. For the most part, they are good corporate citizens who are aware of this, who think it's important to protect their own information, and we believe they are doing what they can to protect the information of others.

The Chair: Thank you.

Mr. Stanton, followed by Mr. Peterson.

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

I want to direct my question to you, Ms. Ireland. In your presentation, you actually were quite outspoken on the issue of what I'll call outsourcing, for lack of a better word, or the notion that companies will take what is in some cases personal information and will use a third-party contractor who may be out of country.

PIPEDA currently allows that under the fourth paragraph of section 4.1 of schedule 1, and essentially says that companies or organizations would have to assure, by contract or other means, that these third-party organizations would provide at the very least a comparable level of protection for those types of services.

We had testimony from the Canadian Bankers Association, for example, that talked about the fact that outsourcing is a reality now, and that it in fact makes business more competitive. By extension, that provides more competitive prices for consumers.

Are you objecting to it just on principle? Could you reflect a little bit on why that would be so objectionable if these third-party companies provide that same level of protection?

Ms. Margaret Anne Ireland: We've had a number of people come to us with a number of concerns on this front. Their concerns have been about things going to another country where the protection may not be as secure. Yes, a company may be responsible here, but are they actually guaranteeing the same level of protection over there as they can here, when they're personally here looking at stuff?

The other thing is that in foreign countries, foreign businesses are subject to their own government's rules. We have had a number of people bring the question to us, especially because the American government has been so aggressive lately about collecting information. They don't want their information going to the United States because they don't want the American government nosing around in their affairs. This may be neither here nor there, but it is a concern of consumers.

Mr. Bruce Stanton: I think we've heard some testimony on that aspect.

On another point, you talked in general terms about tightening up PIPEDA, about making sure protections, penalties, and enforcement would in fact be stronger than those the act currently provides. We heard some other accounts of situations and circumstances in which the current privacy laws don't avail the banks. For example, in one situation, a senior citizen might be under some kind of intimidation to show up at a teller's counter and provide information, with somebody standing right behind them. They spoke quite eloquently, I thought, about the need for a public interest exemption. In these kinds of exceptional circumstances—for example, in the example I mentioned—the bank would be able to contact a relative or someone like that. Currently PIPEDA doesn't allow that.

Would you favour this kind of public interest exemption in a case in which you clearly have a customer who is under some kind of intimidation or threat if they're not ready to disclose that type of information?

Ms. Margaret Anne Ireland: Actually, this is an instance that I can speak to, because I'm a former employee of a big bank. Where I worked, everyone was trained that in that type of instance you were to refuse to serve the customer. You were to send them home. In certain instances, such as with a senior citizen, you were to perhaps suggest that they might want to come back with a family member or some such thing like this. But you were under direct orders to refuse to complete a transaction or to provide a service.

This was where I worked, but I understand the frustration. There were a number of times when I would have loved to be able to phone the son of the 87-year-old man who wanted to buy $50,000 worth of gold and only had $52,000 in his account.

● (1000)

Mr. Bruce Stanton: The hope here is that by doing so, you'd prevent this kind of fraud from happening to someone.

Ms. Margaret Anne Ireland: So I don't know, but I can understand the impulse for that. Is there another way around it?

Mr. Bruce Stanton: That's exactly what we're examining here, and of course there has been a lot of testimony to that effect.

Finally, with regard to CFIB, Ms. Pohlmann, could you shed some light on the experience you saw in Alberta with PIPA? What kinds of barriers did that put on small business in Alberta? We've had a lot of talk about harmonization.

Ms. Corinne Pohlmann: The Personal Information Protection Act in Alberta actually goes somewhat beyond PIPEDA from a small business perspective, because it also has an order-making power. That made it a little bit more intimidating for them to deal with the Office of the Information and Privacy Commissioner, but that's less of an issue. Rather, it expanded to employee information.

In terms of what that did to our membership out there, it was quite amazing how that became the focus for small and medium-sized companies, because except for the 56% with no employees, every company has employees, for the most part. They were very concerned about how to deal with this issue. It caused much confusion. A number of calls that we got were about whether or not they could give a reference or even call about this employee. There were many questions and much confusion around what they could do with their employees or not do with their employees, how it linked to things like human rights and to employment standards.

It was really not well thought out, so we ended up doing a lot of work with the provincial government to try to put tools together and handouts together. There's a lot of information in that province today because of that, but I found that it just added this extra layer of anxiety to our membership in Alberta.

The Chair: At present we have Mr. Peterson, Mr. Tilson, and Mr. Vincent. If anybody else wants to ask a question, please catch the eye of the clerk.

Mr. Peterson.

Hon. Jim Peterson (Willowdale, Lib.): Ms. Ireland, do I read you correctly to say that you want to have much more precise prescriptive rules as to what type of information can be gathered, how long it can be kept, etc.? Would that be the same for big banks, big and small retail stores, and chains versus sole proprietors, etc.? Would those rules have to be tailored to every particular type of business, or would one size fit all?

Ms. Margaret Anne Ireland: I don't know if you need “one size fits all”, but we do need to limit what you can ask for. Does the phone company need your social insurance number?

Hon. Jim Peterson: That's one rule you would say. Phone companies cannot ask for SIN numbers.

Ms. Margaret Anne Ireland: No, do they need it? This is where we have to go. What do they need? What is the minimum they need in order to conduct their business?

Hon. Jim Peterson: There are some companies that may need your SIN number.

Ms. Margaret Anne Ireland: Yes, if you are going to a bank and you have investments and you have interest income, they would like your SIN number so that Revenue Canada can collect money from you.

Hon. Jim Peterson: Then you want a rule that banks can collect SIN numbers but telephone companies can't. Is that the type of prescriptive rule you're talking about?

Ms. Margaret Anne Ireland: I don't think we need to be that prescriptive, but I do believe we need some better guidelines.

Hon. Jim Peterson: Do you have a suggestion as to what they might be?

Ms. Margaret Anne Ireland: We'd really like to see some guidelines around certainly saying you can only collect your social insurance number if it is absolutely required for Revenue Canada purposes. You cannot keep credit card numbers in your data banks for extended periods of time. Once you process a transaction, you don't need that credit card number unless there's an ongoing relationship.

Hon. Jim Peterson: What do you mean by an ongoing relationship? A person may use his or her credit card to purchase an airline ticket every eight months. Is that an ongoing relationship or not?

Ms. Margaret Anne Ireland: Personally I would not consider that to be, but there are people who pay their cell phone bills with their credit cards every month. It is automatic.

● (1005)

Hon. Jim Peterson: That is because they get air miles.

What would be an ongoing relationship?

Ms. Margaret Anne Ireland: If you are doing a monthly charge, that would be an ongoing relationship. I don't think buying an airline ticket once a year could be considered an ongoing relationship.

Hon. Jim Peterson: Then you would envisage a rule that if you do one or more transactions a month you can keep the person's credit card—

Ms. Margaret Anne Ireland: If that is an automatic type of thing, a monthly charge, then I don't think it is unreasonable.

Hon. Jim Peterson: What I'd have to do as a business person, if I got a credit card deal, is check every month, and on the 32nd day, if that credit card had not been used again, I would have to purge my records of that credit card number. Is that what you're suggesting?

Ms. Margaret Anne Ireland: No, but I would think that when a customer cancels their contract, which they have signed for *x* amount of time where you were debiting their credit card, then you would have to purge the credit card.

Hon. Jim Peterson: That's very different from ongoing transactions once a month. I can understand a law that says, if a person cancels a contract to use your credit card, maybe you'd have to get that out of your system, but—

Ms. Margaret Anne Ireland: My wording there wasn't specific. In those instances where people charge their cellphone bills, their gym memberships, those are contracts. They are ongoing contracts where they are being charged on an ongoing basis. As I said, once a year or once every eight months, airline tickets or a trip to the jeans store would not be an ongoing relationship. There would be no reason they would require your credit card to be kept for 90 days.

The Chair: Thank you.

Mr. Tilson.

Mr. David Tilson: The chairman is quite right, I should not speak for them, but my perception is that many of the members of Parliament do not know what this legislation is. Many of us don't even know how to pronounce it. God knows what the French speakers think. They may have a debate in the French language on how to pronounce it.

This legislation has been in the works for, I don't know, a couple of years. Last year the commissioner's budget was $6 million. This year it's $16 million, and that is because of the issue that is before us now. A lot of it is.

The commissioner has come and said that a lot of her budget has to do with education, as have the witnesses. The average person doesn't know anything about this, whether you're a big bank or whether you're a dry cleaner somewhere.

There will be all kinds of amendments. The staff is going to prepare us a list of proposed amendments that have come from witnesses. If the thing is too difficult now, if members of the public find it too difficult now—and this is a question for both witnesses, particularly the Canadian Federation of Independent Business—what will they do when we make a whole bunch of amendments? Will we just drive them over the edge? Let alone in cost, in understanding.... People could be violating the law and they don't even know they're violating the law.

My question for you is this. Taking all that into consideration, and taking into consideration the cost to the government, and taking into consideration the cost of educating individual organizations and their members, whether it is chambers of commerce or independent business or whatever, should our report back to Parliament be that maybe we should just wait a little bit? If we make any amendments at all, maybe we should make it less onerous.

Ms. Corinne Pohlmann: Yes, that is definitely our recommendation. More time is needed to really understand the implications of this particular legislation, as it exists today, on the small business community and on consumers, frankly. I do think education is absolutely the biggest key component of that.

Mr. David Tilson: But I went further. I asked whether we should make it less onerous.

Ms. Corinne Pohlmann: Less onerous? I think there needs to be a simplification in terms of understanding what the obligations are, because the biggest hindrance right now for our members is this policy they have to come up with. They know they have to come up with a policy, a written policy, but they don't know what it entails or how it is supposed to work.

What I think needs to be done is that tools have to be created, or we have to find a way of simplifying it so it becomes clearer what should be part of that policy, and again, without their having to go to a consultant and having to spend thousands of dollars to have them do that for you.

We actually don't mind PIPEDA, to be frank with you, because it is a little more flexible than others. It is a principle approach. It is not prescriptive in nature. But keep it in very plain language.

Our suggestion is to keep it as it is. Let it flow through to Canadian citizens and businesses for a few more years. Allow them to understand what their obligations are. Use the time to educate not just businesses but citizens as well.

I think a big part of this is the fact that individuals want the convenience, as I mentioned before, but they also want their personal information protected. Sometimes you can't have both. You may have to give up one to get the other. I think that's where the challenges lie.

● (1010)

Mr. David Tilson: Go ahead, Ms. Ireland.

Ms. Margaret Anne Ireland: I think, again, that we are almost on the same page. It has to be an educational process. Consumers right now don't know what their rights are. They don't know they can complain. They don't know who to complain to. They don't know what can be done about something if their information is compromised.

In a lot of instances when a consumer's information is compromised, it's not a major crisis. Occasionally it happens that something disastrous goes on, especially in the instance of identity theft. That has unimaginable consequences for an individual's life—for their work, their home, their family, and their marriage. It is very serious.

Do we need more education? Absolutely. We have been doing our best to educate consumers about the act and their rights to privacy, but it's an ongoing thing, and it's slow. It's an uphill battle with this type of thing. What can you do? What can't you do?

Mr. David Tilson: Should the commissioner do that or should we pass this on to the consumers?

Ms. Margaret Anne Ireland: Can the commissioner take on a two-pronged—

Mr. David Tilson: Well, I think the commissioner is doing an excellent job, as best as she can under the circumstances, and she is trying to educate the public. She's travelling around and speaking to groups. The question is this. Is it possible for her to provide adequate education, or should we be saying to groups, independent businesses, chambers of commerce—it could be anybody—"You have an obligation to educate your members as well", and thanking those people?

Ms. Margaret Anne Ireland: Absolutely. I think we can continue on the same path as far as the education goes, with the Privacy Commissioner doing that type of thing. I don't see a reason to take it from her area.

Mr. David Tilson: I wasn't suggesting that.

Thank you, Mr. Chairman.

The Chair: I love to be provocative, Ms. Ireland. But just to give you another chance to reflect, Mr. Tilson's question was rather interesting, because he suggested this: should the committee consider (a) doing absolutely nothing, or (b) making the act even less onerous? And of course, there was complete agreement from the CFIB. As I understood your opening comments, that is contrary to your opening comments. I wonder if you'd like to comment on that suggestion.

Ms. Margaret Anne Ireland: Thank you. We kind of got off on the education end of it.

We don't believe that the act should be made less onerous. We think it should be made clearer, more precise, so that consumers do know their rights and what they can do, where they can go, what is allowed, what isn't allowed. I think a lot of small businesses would like to know what is allowed, what is not allowed, what they can do, what they can't do. Sometimes just knowing "This is what we have to do; okay, that's fine, this is what we'll do".... Trying to muddy around in an area where there are no real rules and you're not really sure what you're supposed to be doing—"Maybe if we do this, it'll be right, but maybe it won't be, and how do we know?"—is difficult.

The Chair: Our final questioner is Monsieur Vincent.

[*Translation*]

Mr. Robert Vincent: Thank you, Mr. Chairman.

I find it very disturbing to hear the comments from consumers and industry representatives. They claim that we may have to wait years to find out what we're going to do about this. I don't see what the problem is.

I think that good old fashioned common sense should prevail. What is personal information? Each of use has a driver's licence. We all have personal information. We know what we're referring to. We also know that certain information such as a credit card number or some such thing should not be disclosed to just anyone.

Therefore, in my opinion, when a consumer discloses personal information to someone, that person should be held responsible. Furthermore, persons or firms to whom personal information has been disclosed become the guardians of that information. If documents are lost, or if some facts are conveyed to other persons, that the individual who disclosed the personal information should be held accountable.

Secondly, the act should contain a provision whereby all costs, including those associated with credit cards, that may have been incurred because personal information was lost should be borne by the company that lost them, and not by the consumer who trusted this business.

What do you think about that idea? The onus should be on the company in question. The owner of a business should be able to protect the personal information of other individuals, of other consumers, as if this was his very own personal information.

An hon. member: Oh! Oh!

Mr. Robert Vincent: I'm sorry for bothering you, but we weren't sure where this was going.

How do you feel about making businesses more accountable for the loss of personal information? Do you feel that they can be made more aware that they have a responsibility here and that they should look at the act to see what they can do? I'd like to get your opinion on this matter.

● (1015)

[*English*]

The Chair: Mr. Vincent, we appreciate the insight we're getting from you on where you might be coming from when we begin our deliberations.

Ms. Corinne Pohlmann: I believe there's responsibility on the business side and on the consumer side. I believe a small business owner collects information that they need to do a transaction that is being demanded by the consumer, and they will use that information to transact that particular service or product. If you start putting limitations on the information they can collect, they may not be able to provide the services or the convenience the consumer demands. I think that's a challenge. I believe most businesses feel they have the responsibility to protect that information. I think we need more time with the current law and education to make sure they understand their responsibilities in doing that.

But I think consumers have a responsibility—and that's where the education component becomes so important—to also know what information to give out and what they perhaps should question. I believe that is also a part of this.

But I do think it's important not to sit there and try to define every piece of information that a business can collect. I think that's a difficult thing to do, because consumers are demanding certain types of information, and it could limit a business's ability to provide the service and may even scare them from providing that service because they can't ask for the information that they need.

[*Translation*]

Mr. Robert Vincent: I think you've strayed somewhat from my initial question.

If, in order to do business with a company, a consumer must provide his credit card number or his social insurance number, then the onus is on the company, and not on the consumer, to keep track of what happens to this information. As consumers, we comply with company requirements. If we knowingly disclose our personal information to this company, we do so believing that it will handle our personal information in a responsible manner. As consumers, I'm sure you have the same expectations.

Hopefully, you won't find yourselves in a situation where, having misplaced your personal information, company officials wouldn't call you for fear their name would be published in the newspapers. Nor should someone be able to steal your identity and make you out to be a criminal. As a consumer, should you assume full responsibility for this situation, or is the company responsible for misplacing this information?

● (1020)

[*English*]

Ms. Corinne Pohlmann: I believe the business has a responsibility and they will do what they can. But if a business loses information because it's stolen from them, for example, it would be difficult for them to know, to go back—

[*Translation*]

Mr. Robert Vincent: If I've entrusted my personal information to the care of your company, I expect it to remain there and not to be disclosed to anyone else. You become responsible for that information.

[*English*]

Ms. Corinne Pohlmann: Yes. And I do believe, unless I'm not correct, the current legislation puts that responsibility onto the employer or onto the business owner, and they are, under current rules, attempting to be able to protect that information as best they can.

When it comes to small business, the fact is that they don't collect a huge amount of information. The information they collect is from people they tend to know and know well. I believe the vast majority of them believe that is information that they are going to protect as best they can. They want to comply by the rules. They understand the need to protect personal information, because they themselves are consumers, and other business is going around everywhere....

I do believe they feel they have a responsibility, and they will do what they can to protect it.

The Chair: *Merci, monsieur Vincent.*

Well, we're at the end of our questioners. I would like to thank our....

Une question?

[*Translation*]

Mr. Christian Ouellet: Yes. Thank you.

Earlier, mention was made of conveying to businesses, both large and small, some knowledge of the act that they are required to enforce. Someone asked a good question on this subject. It was noted that the Commissioner travelled across Canada giving speeches about PIPEDA to keep people informed about procedures that must be followed.

Do you not think the government could take on more responsibility in terms of imparting information about the act to those concerned, using the case of the National Building Code as an example? The federal government publishes the code every five years or so and on that occasion, some representatives crisscross the country to bring people up to speed on any new provisions, even if there are only a few of them.

Some organizations also issue certifications, for example, in the case of ISO, LEED or Novo-Climat in Quebec. For instance, one-, two- or three- hour courses may be given to engineers to provide certifications.

Do you think it would be possible to increase awareness of the act's provisions among small businesses and large companies by providing personal information certifications?

[*English*]

Ms. Corinne Pohlmann: I think that would be a very large and difficult exercise, mostly because most small businesses do not carry that much private information. Groups like ours do a lot of work to try to inform our members. What they need are tools. They do not have the time. When you have three employees and you're the owner, to go out and get certified for two or three hours takes away from what you're trying to accomplish that day, and if you're not dealing with lots of information, I don't see that as being a really useful way of helping businesses get in compliance.

It might be a different story if you were a company that dealt with huge amounts of personal and sensitive information, but I think for the vast majority of small businesses out there, it would be seen as another paperwork burden exercise of government and it wouldn't accomplish what it set out to do, in the way it should.

[*Translation*]

Mr. Christian Ouellet: Ms. Ireland, would you care to comment briefly?

[*English*]

Ms. Margaret Anne Ireland: It's an uphill battle. Consumer education takes quite a bit of time. It has to be ongoing. It has to be repeated. Unfortunately, every year we get a new batch of consumers, and they all have to learn everything from scratch. In this type of instance, we find that consumers frequently, with privacy legislation or some of the other legislation, don't begin to learn about it personally until it affects them personally. If you walk down the street and ask the first 10 people you come to if they know anything at all about privacy legislation or what their privacy rights are, nine and a half of them will tell you they don't know anything.

Yes, we think there should be education—the more, the better; the more ongoing, the better. But as I said, it is an uphill battle.

● (1025)

The Chair: Thank you very much.

Thank you very much to our witnesses. This was an interesting panel. We appreciate your coming and giving us the benefit of your expertise and your opinions and representing your respective stakeholders so well today in our hearings.

Before I adjourn, I have a reminder. On Tuesday we'll have only one witness, and that will be the RCMP. I'm going to call the meeting for 9:15 a.m., so if you're here at 9 and you're looking for us, don't be here at 9. It's 9:15 on Tuesday morning.

Thank you. 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
