House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 027 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Thursday, February 1, 2007

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 1, 2007

● (0905)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): I will call the meeting to order.

Good morning, everyone.

This is meeting number 27, and pursuant to the order of reference of Tuesday, April 25, 2006, and section 29 of PIPEDA, we're conducting a statutory review of a section of the act, in particular.

Today we have witnesses from the Canadian Life and Health Insurance Association Inc., and the Canadian Chamber of Commerce. Welcome.

I guess you know the procedure. Each group will have an opportunity to make a presentation, one following the other, and then we'll have questions from the committee. I'll ask the person who is making the presentation to introduce the people who are with him.

We'll start with the Canadian Life and Health Insurance Association. Will it be Mr. Millette?

Mr. Yves Millette (Senior Vice-President, Quebec Affairs, Canadian Life and Health Insurance Association Inc.): No. We have made a change. It will be Mr. Zinatelli.

The Chair: Mr. Zinatelli, okay. So we'll let Mr. Zinatelli go ahead. Please introduce your colleagues so everybody's name is on the record.

Mr. Frank Zinatelli (Vice-President and Associate General Counsel, Canadian Life and Health Insurance Association Inc.): Thank you, Mr. Chairman and members of the committee.

I would like to thank the committee very much for giving us this opportunity to contribute to your review of the Personal Information Protection and Electronic Documents Act.

My name is, as indicated, Frank Zinatelli, and I am vice-president and associate general counsel of the Canadian Life and Health Insurance Association Inc., CLHIA.

I'd like to begin by saying a word or two about my colleagues who are seated with me at the table.

Dale Philp is assistant vice-president and senior counsel with Sun Life Financial, where she focuses on products and distribution group insurance issues. She is deeply involved with privacy issues in the life and health insurance industry, both within her own company and as chair of the CLHIA's privacy committee, where industry issues of common interest relating to the protection of personal information are discussed.

Yves Millette is the CLHIA's senior vice-president, Quebec affairs. Mr. Millette's lengthy experience in Quebec matters affecting our industry has given him a good familiarity with Quebec's privacy legislation. And of course, as you know, Quebec was the first Canadian jurisdiction to introduce private sector privacy legislation.

We welcome this opportunity to make constructive contributions to the committee as you seek to develop your report to Parliament on this sensitive, complex, and vitally important area.

With your permission, Chairman, we would like to make a few introductory comments. Together with Ms. Philp and Mr. Millette, we will provide the committee with the industry's views pertaining to the PIPEDA review.

By way of background, the CLHIA represents life and health insurance companies accounting for 99% of the life and health insurance in force across Canada. The industry protects about 24 million Canadians and some 20 million people internationally.

For over 100 years, Canada's life and health insurers have been handling the personal information of Canadians. The very nature of the insurance product requires that a large portion of the information exchanged between companies and their clients is personal in nature, and protecting its confidentiality has long been recognized by the industry as an absolute necessity for maintaining access to such information.

Indeed, our industry would not have survived if it were not able to have the trust placed in it by Canadians. Correspondingly, chairman, life and health insurers have taken a leadership role in developing standards and practices for the proper stewardship of personal information.

In 1980 we adopted right-to-privacy guidelines which represented, as far as I know, the first privacy code to be adopted by any industry group in Canada. Those guidelines served the industry and its customers well for 23 years, until they were superseded by personal information protection statutes across Canada in 2004.

In 1991 the industry included a provision in its consumer code of ethics which requires members to respect the privacy of individuals by using personal information only for the purposes authorized, and not revealing it to any unauthorized person.

And a commitment to this provision, by the way, is one of the requirements for membership in the CLHIA.

The committee should also be aware that the life and health insurance industry participated actively in the development of personal information protection rules across Canada such as, for example, Quebec's private sector privacy legislation in 1994.

The CSA model code is now schedule 1 of PIPEDA. The development of PIPEDA itself.... We worked also on the personal information protection acts of Alberta and B.C. and of course on the health information legislation in Alberta, Saskatchewan, Manitoba, and Ontario.

I will now turn it over to my colleague, Dale Philp, to continue our remarks.

● (0910)

Ms. Dale Philp (Assistant Vice-President and Senior Counsel, Sun Life Financial, Canadian Life and Health Insurance Association Inc.): Thank you, Frank.

Thank you, Mr. Chairman and members of the committee. I would like to provide you with a brief background in the next few minutes to the various issues that we have discussed in part IV of the CLHIA's written submission.

Life and health insurers operate on a national basis and deal with a very large number of Canadians, as Frank indicated. In addition, Canadian insurers also carry on their business operations internationally in locations including the U.S., China, India, and the U.K. The operations of life and health insurers cover a variety of personal situations, including financial planning for a potential death, the processing of a disability claim, reimbursing the costs of prescription drugs and other health care expenses, and administration of savings plans or employer pension plans.

These insurance, pension, group benefit operations involve thousands of transactions each day. As these transactions vary in nature, so do the insurers' needs for personal information. We believe a brief description of the parties and individuals involved in our life and health insurance industry might be helpful as context for our issues.

In the group environment, the insurer may insure the benefit plan or only administer an employer's group benefit plan or group pension plan. That's where the employer self-insures its plan.

As well in the group environment, the players then involve the employer, the employee, the employee's dependants, which would be spouse or children, and of course the insurer. It also involves a possible third-party administrator who's retained by the employer to help administer premium payments, etc., and also likely a consultant or advisor to help the employer decide on what should go in their benefit plan.

In the individual insurance world, the players would include the individual policyholder; perhaps a life insured, different from the policy holder; an adviser; and the insurer. In all types of life insurance—individual, group, or pensions—there are also beneficiaries. So you can appreciate the different types of information that would be required to be collected from each of those individual players in the insurance world.

As for the type of information we collect and use under an individual life insurance policy, detailed medical and financial information may be collected when the individual applies for insurance. This is then used to assess the applicant's eligibility for coverage. That file, then, may be relatively dormant for several decades until a death occurs and then a claim is made. In contrast, under most group employee benefit plans, whether insured or just administered by insurers, the insurer is required to collect a small amount of personal information initially, such as name, date of birth, beneficiary designation, and dependents' names. Additional information is collected when a claim actually occurs for the cost of a prescription drug or at the time of a disability, for example. At that time, sufficient additional information must be collected and used to process the claim.

In contrast to the banks, national or international organizations that are provincially regulated are required to contend with an array of privacy legislation across Canada. A transaction that involves the transfer of information from an individual or organization subject to one protective regime—for example, a physician complying with Alberta's Health Information Act—to an individual or organization subject to a different regime, such as an insurer subject to Quebec's private sector legislation or to PIPEDA, will have to meet the requirements of both regimes with respect to consent to disclose under one and consent to collect and use under the other. An employee resident in B.C. may expect that B.C. privacy legislation will apply, but if her employer is located in Ottawa and the insurer processes claims in Toronto, PIPEDA will apply.

In this environment a lack of clarity, gaps, overlaps, or inconsistencies in the legislation can create confusion and unnecessary administrative complexity for life and health insurers, and confusion for their customers. We believe that the coordination or harmonization of the provisions of PIPEDA with privacy legislation at the provincial level would help to avoid such confusion for consumers, organizations, and regulators alike. To appropriately balance the need to protect information privacy with the need to conduct efficient commercial activities, such as providing life and insurance products to Canadians, it is essential that harmonization be given high priority.

● (0915)

While the life and health insurance industry's experience during the three years it has been subject to PIPEDA has been that the current rules are generally workable, a large portion of our specific comments in part 4 of our submission fall under the category of harmonization, with a view to making the provisions under PIPEDA “more practical and more predictable”, to use the words of the Privacy Commissioner.

One of those specific comments relates to the detection and deterrence of fraud. The impact of fraudulent and deceptive conduct on insurance and other financial services can be extremely costly and damaging. Efforts to minimize them are essential. Fraudulent and deceptive conduct can involve a small number of consumers, service providers, and other parties not directly involved with the contract.

Our efforts to control the incidence of fraud in our industry are not in conflict with our protection of personal information, but the current provisions need to be adjusted to make our efforts work better. Specifically, there is a gap in PIPEDA that restricts our ability to disclose information without the consent of an individual for the purpose of conducting an investigation into a breach of an agreement or a law of Canada.

It is the industry's view that instead of, or in addition to, a system of investigative bodies, PIPEDA should be amended to adopt the model used in both Alberta and B.C.'s PIPAs, which allow collection, use, and disclosure of personal information without consent for the purpose of an investigation. In this way, the range of acceptable circumstances as to when personal information can be collected, used, and disclosed during an investigation can be more clearly set out and understood by all parties.

The Chair: Ms. Philp, excuse me. Normally we allow about 10 minutes per presentation; you are at 11 minutes now. I noticed that you have quite a number of other points in part 4. I wonder if I could ask you to highlight the one that you would like to bring to our attention among the remaining ones you haven't discussed, and then close off your remarks. Undoubtedly, we will be able to get to you again in questions, and you, being lawyers, will be able to twist the answers to the way you want.

Ms. Dale Philp: Thank you, Mr. Chairman. I was in fact about to close and hand over the reins, so I'm sorry.

The Chair: That's all right.

Did I cut you off at the knees, Monsieur Millette? You don't have too much time.

Mr. Yves Millette: No. My intervention will be quite short. I will develop only one point, concerning the situation in Quebec.

[*Translation*]

Thank you very much.

Another topic of importance, for the industry, relates to the provisions on individuals' right to access information that concerns them. It is clear that they must have the right to access it, to determine the use being made of it and, if necessary, to correct any inaccurate information.

However, experience shows us more and more cases where access rights are used for purposes that the legislature could never have thought of when the Act was promulgated. Increasingly, companies are receiving detailed, identical access requests, most likely prepared by lawyers, that seem to be "fishing expeditions" to obtain information that would not otherwise be available except through the process of discovery, as it should be.

At present, Quebec's An Act Respecting the Protection of Personal Information in the Private Sector includes a provision covering this type of situation. The second paragraph of section 39 of the Quebec act stipulates that:

> 39. A person carrying on an enterprise may refuse to communicate personal information to the person it concerns where disclosure of the information would be likely to:
>
> (2) affect judicial proceedings in which either person has an interest.

Under this provision, it must be clear that the legal proceeding would be instituted in light of the facts at issue. The industry recommends that the Quebec precedent be used to amend the Canadian act in a similar fashion.

Thank you.

● (0920)

[*English*]

The Chair: Could you just repeat the section number, please, of the Quebec act?

Mr. Yves Millette: It's section 39, the second paragraph.

[*Translation*]

The Chair: Thank you very much.

[*English*]

We'll now hear from the Canadian Chamber of Commerce. Mr. Murphy, please begin, and don't forget to introduce your colleagues.

Thank you.

Mr. Michael Murphy (Executive Vice-President, Policy, Canadian Chamber of Commerce): Thank you, Mr. Chairman and honourable members. It's a pleasure to be here.

My name is Michael Murphy, and I'm executive vice-president, policy, with the Canadian Chamber. Also appearing with me today is Chris Gray, who's a policy analyst with us at the chamber, along with David Elder, who's vice-president, regulatory law, with Bell Canada—a chamber member. Importantly, Mr. Elder is also Bell's privacy ombudsman.

[*Translation*]

As an advocate for Canadian businesses, the Canadian Chamber of Commerce speaks on behalf of a network of 350 chambers of commerce and other business associations representing over 170,000 member businesses.

[*English*]

The chamber is pleased to provide its input on the five-year statutory review of the act. Since PIPEDA was enacted, we have worked closely with our members, local chambers, and boards of trade to ensure that businesses of all sizes understand their roles and responsibilities under the act.

The majority of our members have been subjected to complying with the act since only 2004. We communicate with our members regarding their obligations through a variety of vehicles, and we are always considering how we can continue to better educate all businesses, particularly small and medium enterprises.

To assist our members with PIPEDA, the chamber developed a privacy policy template, modelled contractual clauses, and informed them on how to conduct a privacy audit.

My remarks today will be based on our submission to the commissioner's consultation on the act last fall. We've met with the Privacy Commissioner's office on a number of occasions since the legislation came into force, and we've brought additional copies of that particular submission for your reference today.

[*Translation*]

In general, the Canadian Chamber of Commerce's position on the review of the PIPEDA, the Personal Information Protection and Electronic Documents Act, is similar to the one that other business organizations, such as ITAC and the CMA, expressed to you during previous meetings. The protection of privacy and personal information is a primordial issue for consumers and companies. It is particularly important nowadays because of new technologies that increase the risk that personal information will be compromised.

The adoption of best practices for the protection of personal information is an element of sound business management. A company that uses effective practices in this area increases consumer confidence, and both benefit. From the trade and industry perspective, the Act functions well and requires no amendments at this time. Moreover, most of the industrial sectors and individual companies have just started working within the current framework.

[*English*]

Both business and the Privacy Commissioner's office have demonstrated a solid cooperative working relationship. The structure of the act allows for an effective and workable balance between the interests of protecting an individual's personal information and allowing for business to operate effectively.

In addition, there is a flexibility built into the act that is an important factor in allowing industry to efficiently respond to any privacy issues. PIPEDA, as it currently exists, also has relatively low associated costs and a very efficient complaint mechanism. By maintaining technological neutrality, this legislation also transcends technology change.

I'd now like to turn it over to Mr. Elder to get into some more specific comments from the chamber's perspective that we believe members should consider when discussing the principles of the act.

David.

Mr. David Elder (Vice-President, Regulatory Law, Bell Canada): Thank you, Mike.

The Canadian Chamber and its members believe that Canadian privacy legislation should continue to strike the correct balance between the privacy rights of individuals and the legitimate needs of business to collect and disclose customer information. The flexibility built into PIPEDA has been very beneficial to consumers and business alike during the five years since its implementation.

With regard to the Privacy Commissioner's order-making powers, the current ombudsman model provides an effective manner, in our view, in which to best protect an individual's need for privacy and at the same time address the interests of businesses. This mechanism for resolving privacy issues is critical for consumers, and it is cost-effective. Implementation of an order-making process would require a complete review and overhaul of the role of the Office of the Privacy Commissioner and the Federal Court. Since any such orders would be subject to appeals, this could potentially result in a less timely resolution of issues.

In 2004, under the existing ombudsman model, the OPC increased its emphasis on settling complaints, settling 45% of them without a formal investigation. Changes to the current ombudsman model could significantly adversely impact the ability of the OPC to effect such early settlement. The current model provides the commissioner with a wide range of powers, including complaint investigation and audit powers.

Turning now to the issue of duty to notify, in the Canadian Chamber's view, the current model, again, is operating successfully. I would note that there already exist significant reputational, financial, and legal incentives for businesses to notify customers when there have been serious breaches. Moreover, we believe that the OPC already has the tools to require notification where circumstances warrant it.

Instituting a duty to notify could create a more adversarial relationship between business and the OPC. In addition, imposing a duty to notify on every potential breach could well do a disservice to the very consumers it is meant to protect. This kind of requirement could result in a flood of notices being sent to consumers, desensitizing them to the gravity of a truly serious privacy breach. I believe we've seen this occurring in the U.S.

Given this, the Canadian Chamber does not believe that mandatory breach notification is necessary in the legislation. We would encourage businesses to continue to work closely with the Privacy Commissioner's office in order to identify breaches and to notify those who could be affected by a possible breach in privacy. This flexibility enables notice where appropriate in the circumstances, with no adverse impact on consumers.

I'd also like to note that it would be beneficial for the Canadian Chamber and other business associations to develop a best practices set of guidelines that could be used when breaches in privacy occur. To that end, business groups, including the Canadian Chamber, ITAC, the CMA, and others, are currently developing breach notification guidelines in conjunction with the Office of the Privacy Commissioner. Details on these best practices guidelines should be available later this spring.

With regard to the power to name names, the Canadian Chamber believes that reputation is key for business, and therefore the naming power that currently exists with PIPEDA should not be used lightly. Any proposed changes to the Privacy Commissioner's powers in this regard would represent a fundamental shift in the structure of PIPEDA and would be opposed by the Canadian Chamber.

Take the retail sector, for instance. It is extremely competitive, which is good for consumers, but the naming of names could do serious damage to a company's brand, damage that would possibly be wholly disproportionate to the severity of the breach. Therefore, this power should be reserved for those parties who demonstrate a clear pattern of non-compliance.

If there were to be a routine naming of names, it would not help the relationship between business and the OPC. The Privacy Commissioner herself has stated that she does not require naming powers nor desire them. Most cases can be adequately mediated between business and the OPC.

Given this, it is essential that businesses in all sectors are educated about PIPEDA and their responsibilities as businesses in handling personal information. There needs to be a good balance between enforcement of the law and ensuring businesses, especially small and medium-sized businesses, have a good understanding of PIPEDA so that inadvertent infractions are minimized.

On the issue of transborder data flow, international data flow is an economic reality, and any restrictions on this flow could hinder Canada's competitiveness in the global economy. Companies understand that their business reputations are on the line, and they do not take that responsibility lightly. They remain accountable when information is transferred to a third party for processing.

● (0925)

Policy consistency is essential for efficient transborder data flow, as was illustrated in the APEC privacy framework and the security and prosperity partnership initiatives. The accountability principle that is built into PIPEDA is an effective means of ensuring that Canadian businesses communicate their privacy practices to the public in an open and transparent manner. The accountability principle also requires businesses to enter into contractual agreements with any third-party providers, regardless of where the third party is located. This provides an added level of protection to consumers.

Mike.

Mr. Michael Murphy: Thanks, David.

I'll just wrap up, Mr. Chair, with a quick overview of our conclusions today.

The first one is that there be no changes made to the act at this time and that the commissioner be given the additional time—she talked about five years—she has requested to work with the current act.

Ensure a proper balance is maintained so that the interests of both consumers and businesses are considered.

Maintain the current ombudsman model to effectively protect privacy. With this model in place, mandatory privacy breach notification is not required.

Make no changes to the commissioner's powers with regard to naming power.

Do not place restrictions on transborder data flow that could impede trade and competitiveness.

And we recommend that the Privacy Commissioner's office and other business groups continue to play a strong leadership role in educating and informing firms—and particularly here, small and medium-sized enterprises—and individuals of their rights and obligations under the act.

Thank you, Mr. Chair, for the opportunity to be here today.

● (0930)

The Chair: Thank you very much. You're right on time.

The usual course of action is to proceed with the first round of seven minutes, in the usual order we've agreed to, and then move from there. But before we do, I have one question I'd like to throw out to both of you, as I'm rather curious about it.

Both associations call for harmonization—that makes eminent sense—but you don't think there should be breach notification in certain instances. Just recently, the Ontario and B.C. privacy commissioners jointly released a breach notification assessment tool as a guide for the public and private sector organizations in responding to a breach. Direct notification is the preferred method in the guide whenever the identities of the individuals are known and current contact information is available. That's what the Ontario and B.C. privacy commissioners are recommending.

Do I take it that, because you want harmonization with the other jurisdictions, you're in agreement with this? I'll start with the insurers.

Mr. Frank Zinatelli: Thank you, Chairman.

With respect to breach notification, our position is that there should be a risk-based approach to when notification should be made. In that regard, one looks at the circumstances of the particular breach to determine whether a breach has in fact occurred and whether the event requires notification. In doing that, certainly in the financial services industry, one notifies the Privacy Commissioner; one also notifies our financial regulators to bring them into the picture; and one looks at the particular circumstances of the information that may be exposed.

For example, you do a risk assessment. You determine whether that information can be accessed. If it's in a disk and it's encrypted in such a way that your forensic consultants tell you that the risk is really, really minute, then in consultation with the Privacy Commissioner and in consultation with the financial regulator, you can determine, you can assess whether you should reach out or not.

So we believe that's an approach that works.

The Chair: Mr. Murphy, do you have any comments?

Mr. Michael Murphy: I'll just comment briefly, and I'll ask Mr. Elder to jump in if he would like.

We mention in our brief that we and some other groups are working with the Privacy Commissioner on guidelines in this particular area, and I think, importantly, there are going to be lots of sources of input for that. Clearly, the work that's already going on elsewhere in Canada, in particular with other agencies, the ones you mentioned in B.C. and Ontario, can be one of those inputs.

David, I don't know if you want to add to that.

Mr. David Elder: First of all, I'd confess that I'm not personally familiar with the breach notification tools that you have. There are certainly things that are being looked at within organizations.

The Chair: There's no surprise there. Our witnesses yesterday weren't familiar with them either. I guess it's because it's recent.

I suggest you look at them, because it says:

> Notification should occur as soon as possible following a breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.
>
> The preferred method of notification is direct—by phone, letter or in person—to affected individuals.

That's direct notification to affected individuals whose names are known. That's pretty direct guidance.

Mr. David Elder: It is, and we'll certainly take that into account.

With respect to your question about uniformity, certainly I think we are in favour of a generally harmonized approach. Obviously this doesn't mean that anything that any province does we want to see rolled out across the country.

It reminds me a bit of what my mother used to say: If they jumped off a bridge, would you want to too? So I think we will certainly have a hard look at the guidelines put out by those provinces as part of our ongoing efforts with the Privacy Commissioner of Canada to develop federal level privacy breach guidelines.

The Chair: Thank you very much.

Okay, colleagues. Mr. Dhaliwal, followed by Madame Lavallée.

● (0935)

Mr. Sukh Dhaliwal (Newton—North Delta, Lib.): Thanks, Mr. Chair, and thank you to the delegation for coming over here.

I will carry on with the harmonization as well, because I noticed that you want harmonization between PIPEDA and the provincial legislation.

Can you tell me what are the key changes that you would like to see to bring it on pattern?

Mr. Frank Zinatelli: Thank you.

In fact, if you look at our submission, a number of the changes we recommend are aimed at bringing PIPEDA in line with what has been put in place, if you like, in the third generation privacy legislation that is in place in B.C. and Alberta. As I indicated earlier, Quebec was the first one, in 1994, then PIPEDA in 2001. For our sector, though, it started in 2004. That's when the act began applying to us. But since then Alberta and B.C. have developed what PIPEDA had put in place. So our suggestion is that you look at those newer provisions where perhaps more thought has gone into it, given time and given the experience that they saw from PIPEDA.

One of the areas Dale spoke about is adjusting the provisions dealing with fraud and defining investigation in such a way so that it brings clarity to what the rules are for everybody, because I must confess, I looked at section 7 of PIPEDA, and it's pretty complicated stuff to get your head around. So that's one area.

Another area where the provinces are third generation again is in the area of access. They've gone on to clarify some of the rules in that area, and we have those again in our submission.

Another area that has been talked about and I know this committee has heard about before is when there is a sale of assets or of a business and the purchaser, in doing the due diligence, needs to look at personal information contained by the buyer. So there are provisions in B.C. and Alberta in this regard that may be useful for this committee to look at to determine whether they should be included in PIPEDA, for the purpose of making that area clear.

Another area, and again you've heard about this one, is looking at the B.C. model for their definition of work product and considering whether that should be included in PIPEDA as well.

Mr. Sukh Dhaliwal: So in your industry, the life insurance or the general insurance, what would you call a work-related product and what would you call personal information? How can we distinguish between personal and work-related information? Because everything that you collect probably falls into the work-related information then.

Mr. Frank Zinatelli: Actually, I am going to turn to my colleague Dale to talk about that point.

Ms. Dale Philp: It's in the group insurance world, and I'm going to refer to that frequently, unfortunately, but we collect claims information relating to individuals. The claims are processed and adjudicated internally. Insurers have quality assurance programs in place and review the internal audits of their employees to ensure that claims are being adjudicated properly and processes are being followed. For instance, the SOX audits might involve looking at personal information. I don't think they incorporate personal information into their work product, but there are other processes going on in the business that do not constitute or create a source of information that is not about that individual. It's about the employee who's adjudicating and processing the claim.

Another example might be succession planning in a business. Employees of insurance companies specifically are not caught by PIPEDA. I think generally across the industry the privacy rules are implemented for their employees as well. So employees might say this is personal information about themselves, but I would suggest that succession planning is more business information. It's not information about that individual employee, it's about business continuity. If that individual is not around, someone else will be there to step in.

So those are two examples.

● (0940)

Mr. Sukh Dhaliwal: So every piece of information you collect is a work-related product—there's nothing personal?

Ms. Dale Philp: Every information—

Mr. Sukh Dhaliwal: Yes, because you say it's not about that person, it's about that employee, right? It even comes down to group insurance.

Ms. Dale Philp: No, but the information, when it first comes in the door, is about the.... I guess I'm confusing the employee of the insurer and the employee of a group plan. It's all about that employee in a group plan. It's his name and the name of his dependants, his salary, the nature of the drug he's claiming for—that's his personal information.

On the insurer's side, there might be a review of how that claim information is processed, and it forms another source of information, but it's not about that. I was mixing up the two employees for you. I'm sorry.

All the information we collect in the first instance is definitely personal information.

Mr. Sukh Dhaliwal: Okay.

My question is to the Chamber of Commerce. I've been a member of the Chamber of Commerce for many years. In the riding I represent, Newton—North Delta, all the businesses are either small or medium-sized businesses. I have never seen a letter or a seminar from the local chamber on PIPEDA or anything to do with the privacy legislation. Can you tell me what steps you are taking to inform businesses?

Mr. Michael Murphy: Sure. As I mentioned in my remarks, we have somewhere in the order of about 350 local chambers across the country that are our members, and they're everywhere in all the provinces and territories. As you can appreciate, when you get into the size of an organization like that, you have some pretty significant differences in the size of chambers as well. Some of them have a lot more capability than others.

One of the reasons we focused on this area is that in terms of some of the practical things we tried to do, we actually put information together for our members directly. We did a couple of rounds on this with respect to our members, both corporate and principally chamber, and through them our small business network across the country, to provide them with tools they could use to deal with the act.

We actually put model clauses, contractual clauses, together that we could have inserted into contractual arrangements they may have had with suppliers or customers. We also told them how to go about doing an audit of their own organizations. We also tried to give some basic information.

One of the great strengths of the organization is having access not only to companies like Mr. Elder's in our membership but to Sun Life and many other companies that are very actively engaged. We use some of our bigger members to help in the educational process with smaller members.

The only other thing I'd add is this, and this is not only true of this particular piece of legislation. There's never enough to do or there's never enough that's been done, and there's always more to do in terms of dealing with the small-business community. They have so many challenges, and they form the heart of our economy. You all know the numbers: 95% plus of businesses in Canada are small. They all have lots of challenges in terms of meeting day-to-day requirements. Our goal was to try to tell them through our network what they needed to know about this.

One of the great opportunities about coming here today, quite frankly, is that in the recent weeks we alerted our network that we were coming here. It will give us another chance to put another package together for our members, and we're going to do that.

It's been an effort. We'll never get all the way there.

We're also working with the Privacy Commissioner. She says there's a wonderful need here to keep educating on that side. We agree with that, and working with SMEs is going to continue to be a priority for us.

The Chair: Thank you.

Monsieur Vincent.

[*Translation*]

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

You said earlier, Ms. Philp, that frauds and omissions are detected and that the identity of the organization or company at fault should not be revealed. What do you think of that? Should they be published, so that people across Canada can know that these people have not respected the Personal Information Protection and Electronic Documents Act?

● (0945)

[*English*]

Ms. Dale Philp: I've listened to the translation. I caught on to it late, unfortunately.

I think your question was this: Shouldn't people hear about companies that breach the Privacy Act and shouldn't they be named? Is that the gist of your question? I'm sorry.

[*Translation*]

Mr. Robert Vincent: That's it, yes.

[*English*]

Ms. Dale Philp: Okay.

I think there is a provision in PIPEDA that provides for the publication of a name. When it's in the public interest, that name would be disclosed.

I think that's an appropriate provision when it's found by the Privacy Commissioner—because I don't think she will act outside the limits of her discretion under that provision—that a company is flagrantly abusing the privacy provisions under PIPEDA and the public interest is threatened. Individual consumers are threatened by the breaches that continue by such a company.

I think the provisions in PIPEDA adequately cover the situation where she might make that name public. I don't think we're opposing that provision.

[*Translation*]

Mr. Robert Vincent: What training are your employees given on protecting personal information?

In the case of group insurance, for example, in a factory with 1000 employees on whom you have personal information, how are your employees trained to keep the names of these people confidential?

[*English*]

Ms. Dale Philp: In the insurance area of the industry—and I'm speaking for all of the insurers—there are training programs in place in each of the institutions. I know that at least one member institution of the CLHIA has training in place on a yearly basis for all new employees. They go through a rigorous privacy module, a Breeze module training program. They're scored on how they do on that test, which is given yearly. Frequently privacy tips are left on the Intranet site. There's a business code of conduct that all employees are required to sign every year, which says they have to comply with privacy regulations and only use the personal information they need to do their jobs.

The insurers each have a privacy policy that their employees are bound to comply with. There are individual supplemental privacy processes in place for each area of the company in disability claims, health claims, underwriting, finance, and IT. They all have differing needs to see information and use it for their jobs. There is restricted access to help prevent unauthorized access to information they don't need across the company.

The employees who are adjudicating claims for those thousand group insurance employees are bound by this business code of conduct. They have regular training and their team leads are monitored. Their quality assurance involves continued inspecting or auditing of their compliance with privacy as well.

[*Translation*]

Mr. Robert Vincent: Mr. Murphy, you are the president of the Canadian Chamber of Commerce. Do you think that in the case of companies with five or ten employees, the Government of Canada should provide the training, to ensure these people are aware of the Act? There are clients, individuals who deal with these people.

● (0950)

[*English*]

Mr. Michael Murphy: Mr. Chair, I'll answer the question this way. In terms of the importance of the issue and dealing with small and medium enterprises in Canada, particularly companies—as Mr. Vincent's question points out and I mentioned earlier—as small as five employees, they have lots of challenges.

Regarding the funding of training for companies across the country, I would say not. Through the Office of the Privacy Commissioner, what we have is an opportunity to think about doing a better job. We agree with her that together we can do a better job of getting useful information into the hands of small companies, and there are lots of ways we can do that.

Technology, for us.... Remembering that these companies are all over the country, not just in the big cities.... From our standpoint, we're only three years into a very difficult area with these enterprises that's not unique in terms of the only thing they're thinking about, as I said earlier.

So I wouldn't go so far as to say let's think about a major federal program to start sending people out into companies. I don't know whether you were going that far, but I would say that using the office of the commissioner to think about more outreach for SMEs would be constructive.

[*Translation*]

Mr. Robert Vincent: Does your organization give information to the groups that it represents, that is, that there is an act concerning the protection of personal information and that they are subject to it? When they join your organization, do you talk to them about it? When they become employers, people do not receive a basic kit telling them all the acts they have to respect. Are you in a position to offer some training to members of the Canadian Chamber of Commerce?

[*English*]

Mr. Michael Murphy: Maybe it's just the use of the term "training" here in terms of how we would go about what we do. We have, I think, tools at our disposal, and one of them, as I mentioned earlier, is technology. Our members use our website quite a bit.

We were just talking about this the other day. We were talking about making sure that we continue on so many different files, because the federal government—where I spend my time—touches on all of our members in so many different ways. We're always thinking about the right way to convey important information to our members who are trying to cope with the day-to-day reality of running their business. And what we talk to them about is part of the overhead of running that business. So how do you get useful information into their hands? It's really a question of telling them that we have an office here, nationally, that we can work with, and we're not only happy to do it, we think it's the right vehicle. They should continue to work there and use our technology, including our website, to communicate directly. And, quite frankly, they should use our network, because we have this chamber network that makes us a bit unique in terms of being able to communicate at the grassroots level.

The Chair: Merci, Monsieur Vincent.

The last questioner of the first round is Mr. Tilson, and then we'll go into the second round, starting with Mr. Pearson, followed by Mr. Stanton.

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

I'd like you to talk more about the international aspect the chamber had referred to. I think you didn't want to hinder the economy and transborder transactions, and I couldn't agree more. But there are an awful lot of international transactions that go on with the United States, and other countries around the world, all over the world with computers and outsourcing of information. It's quite remarkable how it's expanded, actually. I quite concur with your observation. We have international insurance companies, companies whose head offices are in other countries. I'm not knowledgeable about that, but there's no question that there are insurance companies that cross borderlines.

On the issue of notification, of course different countries have different laws. Many of the states have different laws about notification. We had some witnesses here on Monday or Tuesday, the bank people. They said that unless there was some reasonable evidence of fraudulent activity, there didn't need to be any notification. There was a story a couple of years ago or a year ago, about some faxes from a bank ending up in a scrapyard in West Virginia. You may recall that story. There were social insurance numbers, home addresses, phone numbers, etc., and detailed banking information. We had a story just a few days ago about a whole bunch of information that just got lost. There's no evidence that it was stolen or used. But again, it included the same detailed information. Then we had the case of HomeSense and Winners—and I'm not criticizing those people—in which information was stolen. Hackers got in.

So my question to you is whether you agree with that philosophy of the banks who say that unless there's evidence of fraudulent activity, people don't need to be notified, or whether you think we need to go further than that. I appreciate that to notify a million people, the postage alone would drive a company crazy. Could both groups comment on that issue?

● (0955)

Mr. David Elder: The banks are maybe in a slightly different position. Perhaps that's why they focused on fraud—because they're looking at people getting access to bank account information and then using that information.

Mr. David Tilson: No, we've got international companies, as in the story of Winners and HomeSense.

Mr. David Elder: Right. But again, that was a story about access to credit card information largely, that people's credit card information was exposed. So maybe that's the focus on fraud.

I would say that, for the purposes of a lot of businesses, that may be too narrow a definition. Part of the problem with having a mandatory breach notification is determining in which circumstances that notification has to occur. And one of the great strengths of the existing privacy framework in the legislation is its flexibility. I think that flexibility needs to be brought to bear in cases of material breaches of information. So first of all, I think the breach has to be material, in some way.

Mr. David Tilson: What about the situation where material is just lost? There was no evidence in the story recently that it was stolen or hacked into; it was just lost.

Mr. David Elder: I guess the question is what was lost, how material was—

Mr. David Tilson: Oh, all kinds of things: clients' names, addresses, signatures, dates of birth, bank account numbers, beneficiary information, and social insurance numbers. It was just lost. They don't know where it went.

Mr. David Elder: It's difficult to speak on behalf of all members. But I think when you have a breach where material information has been provided to third parties, including unknown third parties, and there is a risk that the information could be used for criminal purposes—for identity theft, for God knows what—then I think there should be a notification.

Mr. David Tilson: Let's just localize it to chambers of commerce. People go into stores and their names and credit card information are given. I have no idea what they do with it. Hopefully they're all honourable and they don't keep a record of my credit card information, my address, and my name. I'm obviously on mailing lists. I don't know how they get my name and address, and I'm not even suggesting it came from those people, but somehow I get them. What happens? How did we get on those mailing lists, and what other information do they have about us?

Hon. Jim Peterson (Willowdale, Lib.): David, I gave them your name.

Some hon. members: Oh, oh!

The Chair: Mr. Tilson, I wonder if we could give the insurance industry an opportunity to answer your first question about breach notification, and then we could try to figure out how they get the names. But maybe we could give the insurance industry an opportunity to get in there.

Mr. Frank Zinatelli: Thank you, Mr. Chair.

I might be duplicating some of what my friends with the chamber said, but we believe it has to a risk-based approach. You have to look at whether you're dealing with an incident that has some materiality attached to it. I think you have to have some reasonable grounds to believe that the disclosure has in fact taken place. You're saying something went missing. Well, under what circumstances? Could it still be within the company somewhere and it hasn't gone out of the office? You have to make that determination.

And you have to look at whether there's a significant risk that the individuals whose information you're dealing with could suffer some harm from this. I think you do that by analyzing the sensitivity of the information, whether that information was encrypted and in what form, and by consulting with your regulators to ensure they're aware of the situation and to get some good advice from people who can look at this from perhaps a broader perspective than the company itself. You look at all those factors to determine whether notification should be made.

We discussed this morning that there are a number of guidelines being developed across the country. One of the advantages of not mandating very specific rules in this area is that you can develop guidelines that are similar, apply across the board across Canada, and retain that flexibility to deal with the variety of incidents you could have.

In your introduction to that question, you indicated there were different instances, different possible breaches, etc. They were all different in type, so I think you have to look at all those factors.

● (1000)

The Chair: Thank you.

That was eight minutes, so we'll have to leave the interesting question of how we get on various lists to another round.

We'll go to Mr. Pearson, for five minutes.

Mr. Glen Pearson (London North Centre, Lib.): Thank you.

My question is for Mr. Murphy, if you don't mind.

As a follow-up to Mr. Dhaliwal's question, I understood you have a communication challenge with having to communicate these aspects of PIPEDA to all these various businesses. I would like to look at the communication as it comes the other way. I realize you have to communicate, but if I had a business and I had five employees, for example, my head would be swimming with all this stuff. I don't necessarily have the legal background, and I don't have the legal resources to help me to understand it. I realize you're trying to give tool kits and other things.

I am interested, though, because they are important players in the economy and in the Canadian makeup. Did you provide a venue for information to come the other way? How did they feel about PIPEDA? Did they give insights or ideas as to how they thought it might be improved? I guess the second part to my question would be whether you honestly think they will be able to maintain the focus on PIPEDA and apply it properly, given all the other challenges they have to face.

Mr. Michael Murphy: Yes, it's a very good question, because it is part of the challenge of not only our organization, but all, in terms of dealing with a majority of the members of our group.

One of the good things about being at the chamber and being the policy guy is that I never have to wonder whether I'm going to get feedback from my members on a variety of issues. It's usually coming to me at a rapid rate. It's interesting that this is true regardless of the size of business. That's because of what I said earlier, in terms of the impact—and I'll just deal with the federal level, because that's where we deal at the Canadian Chamber—how much of the day-to-day activity of business government affects in so many ways.

We're not here to discuss the broad principle, but just with respect to this particular legislation—of course, we are just three years in when we're talking about most small companies—we did hear from members on this particular issue as we put information in their hands. We heard it in two ways: not only directly from some of those companies that we get to talk to, direct members of ours, but also through the local chamber network where many of these folks are members.

I won't get into the details of the variety of our communications vehicles, but we initiate feedback ourselves by holding calls with local chambers and others to actually have an opportunity to test the waters on various things that we've done. We put a package together on this particular piece of legislation, and we did that more than once, by the way, because there were different phasings here in terms of implementation. We tried to test the waters.

We don't overburden our members with surveys, the kinds of things where you would mail something out and say, “Could you fill this in, please”, but when we do—we try to do them maybe once or twice a year—we try to capture a bit of an omnibus approach. This is an area that we've tested in the past as well.

The feedback I got, quite frankly, was “You've given us useful tools.” One of the most useful was the contractual clauses that we actually were able to draft with some help from some of the legal members of the chamber, which was very useful stuff. We got very good feedback on that generally.

So is there more to get? There always is, absolutely.

● (1005)

Mr. Glen Pearson: Thank you, Mr. Chair.

The Chair: Thank you.

Mr. Stanton.

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

Welcome to our panel here this morning. It's great to have you with us.

My question is directed to the Canadian life and health insurers. On this issue of fraud detection that you mentioned in your brief, the section you're referring to is paragraph 3(d) of the act, which talks in terms of your ability to essentially disclose, without knowledge or consent, personal information when you see that there might be a potential for fraud or a breach of covenant or a breach of agreement with an insured, in this case.

You talk in terms of there being a gap currently with PIPEDA. I suspect that pertains to the fact that there isn't the term “investigative body”. Are you saying that there is no investigative body to which you could, in fact, disclose?

I wonder if you could give us a practical example to illustrate what this gap is in terms of being able to investigate fraud.

Ms. Dale Philp: It's a good question, and I'm happy to work through it with you.

If we step back, under PIPEDA we have the ability to collect and use without consent when we have reasonable grounds to believe it would be useful in the investigation of a contravention of law of Canada and the information is used or collected for the purpose of that investigation.

Then we move to subsection 7(3), which is disclosure without knowledge or consent, and in this section there is no ability for an insurance company to disclose to anyone other than to a government institution or an investigative body. And yes, you're correct, the life and health insurance companies do not have an investigative body.

The CBA has an investigative body. The Insurance Bureau of Canada may have an investigative body. But the life and health insurance industry does not.

Mr. Bruce Stanton: Just on that point, what about a government institution, or part of a government institution—is there a department or a ministry that is in a position of oversight that could be used in this case?

Ms. Dale Philp: For an investigation relating to fraud under a group members plan, there isn't. We have OSFI and we have the superintendents of insurance across the provinces.

Let me just give you an example of a situation where there might be employee fraud, not insurers' employee fraud but under an employer's benefit plan. The employer may have their health and dental insurance with one insurer and their disability with another insurer, and we have one plan member who defrauds both of these plans. The insurers cannot communicate. They can collect and use the information in their own plans to deal with this fraud, but they can't even communicate with the other insurer to say, “Look, we know we have a common plan sponsor here. Our employer is our client.” They have a rogue employee who's submitting fraudulent claims, and we cannot communicate with them about the identity of that individual. That's where we're stopped, whereas under B.C. and Alberta legislation, we would be allowed to share, for the purposes of investigation and to support and protect our common employer clients.

● (1010)

Mr. Bruce Stanton: What do B.C. and Alberta have that specifically addresses that point?

Ms. Dale Philp: Specifically, they have the ability to disclose without consent. I can give you the section numbers. In Alberta, it's paragraph 20(m). They can disclose the information where it's reasonable for the purposes of an investigation or a legal proceeding. The similar section in B.C. is paragraph 18(1)(c). In contrast, in PIPEDA we're restricted; we have to share with an investigative body.

And then I think somebody the other day, in the submissions by the banks, made a submission that even investigative bodies can't communicate with each other. So it's just a clear little gap.

Mr. Bruce Stanton: Very good.

Do I have any more time, Mr. Chair?

The Chair: No.

Mr. Bruce Stanton: That was clear—always very straight to the point. Thank you.

The Chair: Just on that point, Ms. Philp, if you have a husband and wife, and each of them has a different employee plan, and let's say there's a dental claim, and the husband puts in a dental claim. You know on our form there's a question “Are you covered by some other insurance company, yes or no?” Suppose the husband puts in “No” and the wife puts in the claim for her husband. Same claim, two different insurance companies. There's no way those insurance companies can know—or can there be? I'm asking the question, is there a way for those two separate insurance companies to figure out that the same claim has been put forward and paid twice?

Ms. Dale Philp: That's a great example of a situation where we cannot communicate. We cannot say "We have Joe Smith, and we know that Irene, his wife, has a plan under the insurer across the street, and we think that the same claim is being submitted under both plans."

Ultimately, it catches up, and we'll work with that person under our plan and say, "Sorry, you're covered under another one." We'll work through it indirectly.

The Chair: But on that example, could you not go to law enforcement with your suspicions and ask them to investigate? And by the way, how would you have a suspicion if you can't get the information?

Ms. Dale Philp: We may get suspicions, they may come up through tips. People may call in. We may see an irregular claims pattern. From time to time we do look at claims. I don't know exactly how we would. I can find out, because I know we've had that situation and I don't know how we learned of it. I can't tell you, but I could let you know about that, if it helps.

The Chair: Maybe it's not a good idea to do so, because then someone will know how to do it.

Ms. Dale Philp: That's true.

The Chair: Anyway, the point I'm asking is if you had such a suspicion, you could bring that suspicion to the attention of the police and ask the police to further investigate, could you not?

Ms. Dale Philp: We could. We can hand over our file. There'd be more evidence for the police if they knew it was happening. They'd have to go and then ask for information from this other insurer. The other insurer might say, "You have to serve us with a subpoena. We can't disclose personal information unless there's...."

The Chair: Understood. Okay.

[*Translation*]

Mr. Vincent, you have five minutes.

Mr. Robert Vincent: Thank you.

I would like to go to page 13 of your submission. It says:

> A question that has been much discussed in recent times is whether organizations that suffer loss or theft of personal information should have a legal duty to report the loss or theft. It is worth noting that the openness principle (Principle 8 of Schedule 1) already suggests that an organization has responsibilities along these lines. Consequently, the industry is of the view that no specific legislative provision is needed at this time.

Here is my first question. Does this mean that if you lost information or had it stolen, it would not be necessary to tell anyone at all, that the industry would decide what to do about it?

Continuing on:

> The industry supports a risk-based approach to notification, where the need to notify and the method of notifying the individual are proportional to the risk of harm that may be experienced by those whose personal information has been compromised

My interpretation is that if you lose my personal information or have it stolen, you are going to decide for me whether I am going to be harmed by it. And reading on:

> Where the breach is material; where the organization has reasonable grounds to believe that disclosure of personal information to unauthorized individuals has taken place; and, where the disclosure presents a significant risk of harm to individuals (e.g., identity theft or fraud).
>
> In applying such parameters, an organization would perform an analysis (taking into consideration the sensitivity of the information, whether that data was encrypted, etc.) with a view to determining whether notification should occur and, if so, how notification should take place.

If I understand correctly, regardless of the situation, it is you who will decide if it is necessary to advise me if personal information is lost or stolen.

● (1015)

Mr. Yves Millette: I think it is necessary to exercise some discretion. We were talking earlier about encrypted information. Under those circumstances, since it is not useful to anyone, it might be more damaging to inform the public than to keep the information confidential. That's one factor.

Mr. Robert Vincent: It's more damaging for your organization.

Mr. Yves Millette: For consumers as well. It creates uncertainty for them.

Besides, we were talking earlier about the information found on all the telemarketing lists. If it is already on all these lists, it may not be necessary to make a specific disclosure.

That is the background to our decision to support risk-based decision-making. The risk can be real, non-existent or insignificant. In some cases, information can create more problems than it solves. Moreover, as we say in our submission, it is not the company alone that makes the decision. It consults the information commissioner and regulator.

Mr. Robert Vincent: That is not what I got out of reading your submission. I'm not trying to corner you: I'm just trying to understand. We have all insurance. I would like to be sure that I would be told, without you deciding whether it is appropriate, if my personal information is lost or stolen, or sent to someone by one of your employees. It might not be good for your image. The fact remains that I might consider that information to be crucially important. The potential for identity theft might be greater than you think.

Mr. Yves Millette: In fact, the company doesn't decide, it refers it to the commissioner.

Mr. Robert Vincent: I see no mention of the commissioner in your submission. In fact, it is about the organization that loses the personal information, it says that the organization must analyse the situation, but there is nothing anywhere about transmitting this information to the commissioner. You decide whether it is appropriate or not, whether the loss is serious or not. I don't see anywhere that you are going to advise someone, but I do read that you are going to decide about what you have said. I can only read what is written in your submission. You have to explain to me whether my personal information is safe with you or not.

Mr. Yves Millette: Your personal information is safe with us, no question. I understand that you would like a public notice every time there is a possibility of an information breach.

Mr. Robert Vincent: Or that it be sent to the commissioner, as you said. A notice should be sent immediately to the commissioner, who could decide whether that information should be sent to the victims of the theft, for example, or whether there should be a public announcement that someone has lost the information. The commissioner could decide, rather than the organization. What do you think?

● (1020)

Mr. Yves Millette: I think that's a good question. Your suggestion is probably very interesting. I think that, in any case, an insurer will do that if there is a serious information breach. It is clear that it will have to make risk-based decisions, if only with the insurance regulator, for example. The superintendent of financial institutions monitors risk management. There are specific risk-management regulations that apply to insurers. At that point, the superintendent of financial institutions would have to be advised, if there is a dangerous breach, if there is a threat to the company's reputation or a business risk. All these things must be revealed to the regulator.

[*English*]

The Chair: Okay. Merci.

Mr. Vincent asks a very important question, which I want to be sure we have an answer to.

The industry supports a risk-based approach to notification. Who makes the determination of the risk? Is it the company alone, is it the company in conjunction with the Privacy Commissioner, or is it the Privacy Commissioner who institutes it? In other words, who decides that the breach is material?

This is what Mr. Vincent was asking, so let's get a clear answer.

Mr. Frank Zinatelli: Mr. Chairman, the decision as to whether the breach is material is made by pooling the information and resources from all those groups, not only from the Privacy Commissioner and the company, but also from forensic accountants, if it's appropriate, and our financial regulator, whom we would inform at the same time as we would the Privacy Commissioner.

One of the concerns in this area is that if something very specific is put in the legislation that ties your hands in all circumstances to having to follow the same procedure, you may end up doing what is right now in the circumstances, but have to follow that specific set of rules.

I think those rules are followed; that due diligence, if you like, is done in determining whether a notification is made. But it's in conjunction, by everybody pooling their efforts.

The Chair: I understand your point that enshrining something in legislation may be too confining, depending on the circumstances. I think we all understand that.

Mr. Frank Zinatelli: Yes.

The Chair: But just to be clear, isn't it your position that the company and the company only should determine whether the breach is material? Is that right?

Mr. Frank Zinatelli: There is all kinds of pressure on the company to listen to what the financial regulator says, to what the Privacy Commissioner says, and for reputational reasons, etc. But ultimately, under the current rules, it would be the decision of the company.

The Chair: Well, that's exactly the point. Right now, it is the decision of the company and the company only, unless someone complains and involves the Privacy Commissioner. That's exactly the point.

And that's the answer, is it not?

Mr. Frank Zinatelli: But I just want to add that in the normal course, whenever I've heard of any instances in this regard, the first step that our companies take is to talk to the Privacy Commissioner and our regulator.

The Chair: That's understood. I'm just trying to figure this out. In a bottom-line scenario, it's the company that decides what is a material breach—yes?

Mr. Frank Zinatelli: Under the current rules, that would be my understanding of it.

The Chair: Yes, as it would be mine. Okay.

We go to Mr. Van Kesteren, followed by Mr. Peterson, followed by Mr. Tilson.

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

I am of the opinion—and I said this yesterday too—that the insurance industry probably could have written a book on privacy. I think you have done a good job. I think there is always room for improvement. We've heard some great questions and we need some direction in certain areas.

I am concerned about one thing, though. I stated yesterday that most of this has come about because of the information age and things that none of us expected or anticipated.

I want to direct a question, and I think I should direct this question to you, Ms. Philp. With Sun Life, for instance, or the insurance industry generally, when you have overseas ventures like in China.... I understand in that particular case that the advantage you have over other companies is that you have an integrated system. In a case like China, where they take 50% ownership or the government is a partner, what kinds of safeguards do you have if you have an integrated system? For instance, in the government here, I think Sun Life has our insurance policy. What do we have for safeguards that some of that information isn't going to get out?

● (1025)

Ms. Dale Philp: I'm not exactly certain what systems we share with China, if any. I think it's a totally distinct business operation over there. I'm virtually certain there is no sharing of our access to information in Canada with China, other than maybe on a business level for directors and with the financial results of the company, as opposed to personal information.

As for the public service health care plan that is administered by Sun Life, there is no access to information from anywhere outside Canada to information under that plan.

Mr. Dave Van Kesteren: Okay.

The other area is that you mentioned something about requests from lawyers. I suppose they would access it through the Access to Information Act. Some of this information is being used in trial cases—did I understand that correctly? Is that something that should be addressed, perhaps through the Criminal Code, so that if information is obtained through the access to information process, it would not be admissible in court? Is that something you have looked at?

Ms. Dale Philp: Maybe Frank can answer that one.

Mr. Frank Zinatelli: It really is something that needs to be looked at in the context of the privacy legislation, because that is the place where the right of access is provided, with a list of exemptions. In our brief we were pointing to the Quebec example, where they have looked at that situation and indicated that not all of that information should necessarily be accessible all the time. You've got to look at circumstances where that information might lead. That is not the purpose of the privacy legislation, at least in Quebec. So they have moved a little bit further to restrict when that information can be disclosed. I see the parallel being in PIPEDA, as opposed to any other statute.

Mr. Dave Van Kesteren: So the solution is just to change some of the rules?

Mr. Frank Zinatelli: Yes, and to look at the Quebec rule in determining that and to try to bring this in parallel with the rules there.

Mr. Dave Van Kesteren: Okay, that's all.

The Chair: Mr. Peterson.

Hon. Jim Peterson: Mr. Zinatelli, you said that in practice, if there is a breach of privacy, the Privacy Commissioner is notified by companies in all circumstances. Do you think we should make that requirement mandatory?

Mr. Frank Zinatelli: Actually, in the circumstances I am aware of, there has been notification. Should it be made mandatory? I think whether or not something like that should be made mandatory is a question that should be looked at down the road. I'll give you one of the reasons.

Hon. Jim Peterson: But not today.

Mr. Frank Zinatelli: And the reason for that is that all sorts of rules about notifications are being developed by various parties, such as the Privacy Commissioner.

We've heard from the chairman of two other instances where I believe Ontario and one of the other provinces—

The Chair: B.C.

Mr. Frank Zinatelli: —have come up with these guidelines.

So let's see, in the coming period, what the consensus is as to what those rules should be and then let's see.

Hon. Jim Peterson: I agree. Thank you.

Ms. Philp, the main thrust of your presentation was on how we can benefit from harmonization. Do you have any estimate of how much time is wasted or is made redundant by overlap and duplication with provincial laws? Do you have any horror stories? How bad is the overlap and duplication? I'm sure you see a lot of it from your vantage point in the company.

● (1030)

Ms. Dale Philp: I do, and I see it when we have a situation of employee fraud, not our employee fraud, but an employer's employee fraud. And my first question is what province are we in, is it Quebec, is it B.C., or Alberta, because I want to know how we have to deal with that information and if we need to get the consent of the individual to share with others.

And there is another situation where we're administering the self-insured employer's benefit plan. We're not the insurance company, we're the agent; we're administering. When there is an employee fraud—their employee's fraud—we, without consent, can't share that information with the employer unless we're in Alberta or B.C.

Hon. Jim Peterson: Thank you.

I want to say how much I appreciate your specific examples of how we could eliminate overlap and duplication.

The chamber said to make no changes to PIPEDA at this time. Would you modify that to allow us to make changes of the nature outlined by the insurers, with respect to overlap and duplication, to move toward harmonization?

Mr. Michael Murphy: This is an area that was of pretty big concern to us, particularly at the time B.C. and Alberta were looking at their legislation, which didn't exist until we got going at the federal level. It was about the same time.

I heard from members all the time about how worrying this was going to be for them. There are examples specifically, and I think you've heard it expressed very well here of where there may still be some concerns. But on the broad level, is that concern still reflected in my membership, broadly? No, it's not. So I don't have anything specific to suggest, and I certainly don't want to take issue with what our friends in life and health insurance are saying.

David, do you have anything to add? No? Okay.

The Chair: Thank you, Mr. Peterson.

Mr. Tilson, and we'll follow Mr. Tilson with Mr. Dhaliwal. That's the last person I have on the list at this time.

Mr. David Tilson: Okay, thank you.

To the Chamber of Commerce, I represent a community known as the beautiful town of Orangeville, Ontario.

The Chair: Orange County, did you say?

Mr. David Tilson: One of your members, one of the members of the local chamber of commerce there, knew I was on this committee—and I've been on it for a little bit of time—and he said to me that he found the provisions of PIPEDA an absolute pain. He said that it's an example of.... For certain promotions he has, if someone does a certain amount of business with him, he has the names and addresses and credit card numbers and all kinds of information about people. So each time he does a promotion for his customers, he has to get the consent of his customers.

My question is whether the Chamber of Commerce, locally or provincially or nationally, has done a cost-benefit analysis on the business compliance of PIPEDA.

Mr. Michael Murphy: The short answer, Mr. Chair, is no, we haven't done anything like that. And that doesn't make implementing this act and its impact on business any different from most pieces of legislation.

Mr. David Tilson: Well, to be fair, he's done it for a while, and he's used to doing it, but when he first had to do it, he said what he had to deal with was terrible.

Mr. Michael Murphy: So many businesses hopefully doing so many different things to attract customers is all part of the thrust and cut of a vigorously competitive marketplace. Dealing with legislation, I have to say, is not a complaint I've heard from a bunch of members. Is that something that has become a theme?

Mr. Gray, you'd probably agree that it's not something we've heard from members on a repeated basis. I don't want to diminish the concern that was expressed by that particular company, but that wouldn't be a general statement, I would say.

Mr. David Elder: Sorry, but if I could just jump in, I know Mr. Nelson too. I don't know the particular facts of your constituent, but I'm not sure he would necessarily have to get consent each and every time he ran a promotion. I think there are ways to do a more global sort of consent.

Mr. David Tilson: He can get a blanket consent. It's not a question. What do you think of those things?

Mr. David Elder: Yes, and I'm sure if he contacted his chamber, we could help him out.

● (1035)

Mr. David Tilson: Mr. Murphy, I think it was you who indicated that the commissioner has come to us several times and has said that a lot of what she does is educational for the public. That's what a large portion of her budget is for: educating the public on this whole topic. I believe you said you had some information on your website about PIPEDA.

Mr. Michael Murphy: Yes, that's correct.

Mr. David Tilson: Is it there right now, as we speak?

Mr. Michael Murphy: Absolutely, yes.

Mr. David Tilson: Do you have a link to the Privacy Commissioner?

Mr. Chris Gray (Policy Analyst, Canadian Chamber of Commerce): If I could just cut in, Mr. Tilson, Mike and I spoke about this yesterday and we're in the process today. The information is there, but we're going to make it a little easier to find for members, stemming from our participation here. We're going to have a direct link to the Privacy Commissioner's website, where there are a lot of good tools for members to use. We also have our previous information that Mike referred to— our contractual clauses and our templates—and which will be easy for members to find.

If I could just go back for a second, I handle the privacy matters with the chamber. Even tomorrow we're meeting with ITAC and the CMA to discuss better education principles and how we can work together there, as well as starting to think about these draft breach notification guidelines.

Just to reiterate, members, it's a two-way street. We have a biweekly newsletter that we send out, and we're always updating members on what's happening in regard to privacy and other issues. My name and the files that I handle are right on the website as well, so they can always give me a call, especially the small members who don't have the resources to do it themselves.

Mr. David Tilson: And in insurance, do you do education on your websites?

Mr. Frank Zinatelli: We work with our member companies. In fact, one of our raisons d'être at the association is to ensure that our members are aware of developments in the privacy area. In fact, when the legislation first came in, both in 1994 and again in 2001, and when the Alberta legislation came in, we prepared, for example, Q's and A's in cooperation with regulators and by working with our member companies, so that our companies would have the right information, the up-to-date information, so that they could then reach out to their clients, as Ms. Philp was indicating earlier. Educating our members is really one of our important functions.

Mr. David Tilson: This line of questioning was following along Mr. Pearson's questioning about feedback that you've had. I appreciate that you philosophized about whether your members, from both groups, have indicated concerns. You've expressed all those.

The Chair: Mr. Tilson, you're at almost six minutes now.

Mr. David Tilson: Okay.

The Chair: Mr. Dhaliwal, we can put you back on if you want to ask another question.

Mr. Sukh Dhaliwal: Thank you, Mr. Chair. My question is to Mr. Murphy and Mr. Gray.

When you put these recommendations that you don't want any changes or whatever these eight recommendations are, are they just from your organization, or have you taken the other small chambers into consideration as well? Had you asked for their feedback when you came up with these recommendations?

Mr. Michael Murphy: The thoughts we've expressed here stem from a fundamental belief that in coping with legislation like this.... I make two points. First of all, for most of our members, and that would certainly include the smaller members, we're only three years in, and in the scheme of legislative enactment in Canada that's very young.

I would couple that with the Office of the Privacy Commissioner's own comments about...and I think the arrival of the current commissioner was almost coincident with that phase, in January, 2004, where the bulk of companies in Canada got captured by the act.

As the commissioner herself has indicated to you, there are lots of preoccupations there for her, to do things in the office other than get on with the core work of implementing the act.

So it's early days, and I think that's the philosophy behind the recommendations.

As to our view on whether this is something that's shared across our membership, I would say it is, very strongly. This is a case where three years in on any bill, and particularly one that affects so many of our members, is really early days.

To change it today, when you're still in the educational phase for a lot of them in terms of their building themselves up to deal with the important elements of the act, I think is going to complicate life a lot more than we need to at this stage.

● (1040)

Mr. Chris Gray: Let me just add to what Mike said that the September submission we gave to the Privacy Commissioner is based upon a policy resolution that the Canadian chamber adopted at its 2005 AGM, which all the local chambers come to. So that's adopted by 250-plus grassroots members. We're very grassroots-driven, and with regard to developing this, that was the basis of it.

But we also have an internal chamber committee that deals with privacy matters. Of course, I get their feedback—from our corporate members as well—and that's how this was rounded out in late summer. I will admit it was difficult to get some people in the late summer working on this file, but it encapsulates views everywhere from the chamber's views to those of our corporate members and our other associations, such as the Retail Council of Canada. They've all provided input into this concise document.

Mr. Sukh Dhaliwal: My follow-up question, Mr. Chair, is to Mr. Gray.

It's good that you have on your website the information about PIPEDA, but as Mr. Pearson said, all these small businesses have their own challenges to establish themselves, because they are the backbone of any community.

Is there a way that you can put this information in a very simplified way into layman's language, so that they can go to the website and access that information and familiarize themselves?

Mr. Chris Gray: It's a very good question. Mike Murphy and I were just discussing this yesterday. As we navigated our website, it wasn't as easy to find as we wanted it to be. So we're in the process today—and by Monday, hopefully, we'll have it up there on the main website—of putting up information indicating that our templates are there and showing what we set out previously. Also, a link to the Privacy Commissioner's website will be right on our main website. That will help members to better engage this.

Stemming from this, Mike also mentioned that we're going to be redoing an awareness campaign—we have a biweekly newsletter.

So we try to reach out as much as we can. That being said, in my experience with the chamber in the past couple of years, it's fairly rare that I get questions from members on this, so my understanding is that they understand their obligations and responsibilities under the act.

Mr. Sukh Dhaliwal: I appreciate all the work that chambers do, but this is one area where I personally, being a small business person and a member of the Chamber of Commerce, think we were not able to get the information to the small businesses. Maybe you can put in a link to the local organizations as well, such as local chambers of commerce, so that they can copy that information onto their websites also. That will be a positive step to informing the small businesses.

Mr. Chris Gray: Thank you. We'll take that recommendation.

Mr. Sukh Dhaliwal: Thank you very much.

The Chair: Mr. Gray, I don't think you should assume—this is my own personal opinion—that because you don't get a lot of questions, everybody understands it. I think it may very well be the opposite. If they don't understand it, they don't go to it, and so they don't pay attention to it and therefore have no questions about it.

Mr. Chris Gray: I agree. It's true that we don't get a lot of questions on it, but just going back to Mr. Dhaliwal's questions, we will be redoing our communications on this file, if you will. I'm almost hoping that more discussion on it results from that, so that more organizations—especially the SMEs—can understand. If they have questions, they can—please—give us a call, and we can help them.

The Chair: I'm not a web designer, and in fact I must admit that I rarely use my computer. But don't call it PIPEDA, because no one knows what that is.

Mr. Chris Gray: Yes.

The Chair: Call it “privacy issues” or something.

Mr. Chris Gray: Yes, that's what we have called it.

The Chair: Okay. Good.

Mr. Tilson.

Mr. David Tilson: Thank you.

I would like to ask a question, at the risk of the chairman accusing me of cross-examining you.

The question has to do with it being at a company's discretion, as he tried to make clear, for whatever reason, as to whether or not customers or clients would be notified. That's the understanding of both groups, just so I'm clear.

Mr. David Elder: Actually, if I could add a gloss to that, I would say it's typically the decision of the organization at first instance, but it's ultimately a determination to be made by the Privacy Commissioner of Canada.

Mr. David Tilson: But there's no obligation to tell the Privacy Commissioner.

Mr. David Elder: Not immediately.

Mr. David Tilson: No, never.

● (1045)

Mr. David Elder: Well, in many cases, it's certainly not a course of action that we would recommend.

Mr. David Tilson: But no one will ever know.

Mr. David Elder: If you look at the act, it's the same for determining what form of consent to use. It's the same for determining how much access to give someone to personal information that you have on file. It's the same for determining what constitutes personal information in the first place.

In all of those cases, the organization by necessity makes the initial determination. But the Privacy Commissioner is there to ultimately make that determination, if called upon, and to publish those findings such that all organizations can learn from those and can benefit from that guidance in going forward.

Mr. David Tilson: I understand. These recent cases that have been in the media, and the finding of information in the scrap yard in West Virginia a year ago, were so extreme. If they weren't talked about and it ever got out, it would be terrible publicity for the companies, banks, or credit companies. They did the right thing. But I assume there are situations of a much lesser degree where a company makes a decision, for whatever reason, whether or not to advise anybody, whether it be the Privacy Commissioner, the individual client, or the customer.

It leads to the question on the international business you mentioned, with China or other countries. Any foreign countries having subsidiaries here or doing business in this country, whether it be insurance or otherwise, do not have to talk either, do they? If they are notified of some breach, there are no repercussions if they don't tell anybody. Isn't that right?

Mr. David Elder: I'm trying to understand your examples.

Mr. David Tilson: All right. Obviously, I'm hung up because of what's recently happened on this whole issue of notification. There were individuals who found vast amounts of personal information, everything from names to social insurance numbers. Should people be notified?

The answer that seems to be coming out is that if there are signs of fraudulent activity, yes, we're going to talk. But other than that, there's no obligation and it does not even create an obligation. There's no obligation to tell the Privacy Commissioner, clients, or customers, whether you're a foreign company or a national company.

Mr. David Elder: I think that in many cases there may well be an obligation.

Mr. David Tilson: What's that?

Mr. David Elder: The Privacy Commissioner is working through some of these schemes right now.

As we mentioned, we're working with her office to develop a set of brief notification guidelines. But it's open to the commissioner to issue findings on a case-by-case basis as these things come up. I think we've recently seen that she initiated an investigation into T.J. Maxx.

These things will result in a finding that says in this kind of a case, when this much information goes forward, you have a duty to notify and this is what the notification looks like. I think those tools are already there.

Mr. David Tilson: Okay. In any event, your summary is to let it go a little bit, and hopefully, whether it's through guidelines or code ethics, which someone talked about, you'll want to try that process to see how it goes before we start putting too much into legislation.

That's the general position of both groups. You're both shaking your heads, yes.

Mr. David Elder: Yes.

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

The Chair: Thank you, Mr. Tilson.

Our last questioner will be Monsieur Vincent.

[*Translation*]

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

I am going to continue in the same vein as just now. I am confused. If there is a theft or something happens in one of your organizations, you feel you have the leisure to reveal it or do something, be it at the level of the Canadian Chamber of Commerce, businesses, or, as I understood it, insurance companies.

Could the Act not state that, as soon as a party realizes there has been a theft or something of the sort, it must advise the commissioner, who conducts an investigation to determine the repercussions of such an event on the personal information of people who deal with your organizations?

Should there not be a section in the Act that encompasses this type of problem, rather than leaving it to the organization to judge the appropriateness of revealing it?

Mr. Yves Millette: In general, that remains a business risk. I think that the company must ensure that revealing information does not create more problems than it solves. In that respect, many of these things relate to the daily routine. Procedures will be adopted automatically and firewalls will be adapted as a consequence. Companies have risk-management systems, and these things will therefore be contained very quickly. The procedure will become very cumbersome if there is a requirement to notify the regulator every time. In every case of the slightest importance, the regulator will be involved.

● (1050)

Mr. Robert Vincent: I agree with you. If you think it is important, the commissioner could decide, without making the process cumbersome and endangering the company, that it's all right and that the matter won't go any further, that there is no need for disclosure. However, that a third party make a decision in a given matter without leaving it to the company itself—

I understand your point of view. It risks being more damaging for the company, but not the consumer. Consumers who trust a company can turn over personal information. I am not talking just about you, but about all the people who trust that company and who know that their personal information is safe. Yet, we have seen today that it is no longer that safe.

Mr. Yves Millette: The point of our recommendation was to examine these things and, through directives, to establish a procedure that would benefit everyone and not go completely to the other extreme, of having to inform the commissioner of every situation, which could be counterproductive for the conduct of business.

Mr. Robert Vincent: OK.

Earlier, I asked Mr. Murphy to talk about the Internet. In 2006, the Canadian Internet Policy and Public Interest Clinic published a study of 64 on-line retailers to see if they were complying with the Act. The study revealed that a certain number of retailers were not respecting the fundamental requirements to protect personal information.

Do you think that the problem this study brought to light reflects the fact that companies are not aware of the Act's requirements, downplay it and hope they don't get caught, while continuing to operate in any old fashion?

[*English*]

Mr. Michael Murphy: This is the central question in terms of the educational component here in dealing with companies, specifically in trying to raise the bar, if I could put it that way, on knowledge, something that the Privacy Commissioner has said is one of the objectives for her office, and I think she'd like to have more resource power there dedicated to doing more of that rather than some of the things that she had to do earlier on in her term.

In a perfect world, you don't have anybody who's missing in terms of understanding their obligations under the act. I mean, are we in that situation today? I'd never want to make that statement, given the number of businesses that are out there, but from the standpoint of where we are, I think from the standpoint of companies in Canada and coping with this legislation, I'll use the words of the Privacy Commissioner, that the system is working well. I think she has not only said that here, she has said it elsewhere. That's the fundamental premise on which we start the discussion here. So I think we start from a position of reasonable strength and look for ways to continuously improve.

I'll leave it at that, Mr. Chairman.

The Chair: Okay, that's a good place to leave it in completion.

Madame Philp and gentlemen, I would like to thank you on behalf of the committee very much. I'm sure you can appreciate that there's a great deal of interest in this subject matter by the committee members, based on the questions you had to field today.

Good luck with your redesigning of the website, and good luck with your members. I know if I were in small business, this particular statute, among many others that governments impose on businesses, would be perplexing to me. So many thanks for appearing today and for giving us your advice.

Members, our next meeting will be on Tuesday, at 9 a.m. It's very likely I will not be here, so I've asked Mr. Tilson to take the chair on that day. Thank you.

I adjourn the meeting.

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
