House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 022 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Wednesday, December 6, 2006

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Wednesday, December 6, 2006

● (1535)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): Good afternoon, ladies and gentlemen.

We have quorum, so I'd like to call meeting number 22 of our committee to order, continuing our statutory review of PIPEDA, particularly part 1.

We have a number of witnesses before us today. I think what I'd prefer to do is let the witnesses introduce themselves, other than the main speaker for each one.

For the Canadian Internet Policy and Public Interest Clinic, we have Ms. Lawson, executive director, I guess speaking for the group. Welcome.

From the Public Interest Advocacy Centre, who will it be? John Lawford? Where are you?

Welcome. We've received your material.

Oh, there's another person? I'm sorry. From the Marketing Research and Intelligence Association, it's Mr. Stark. Welcome.

And Mr. Brendan Wycks? I have an old sheet. It isn't my intelligence; I just have an old sheet. All right, I apologize for that.

Anyway, please feel free to introduce whoever's up there, reintroduce yourselves, whatever; it won't count for your time.

What I wanted to say was that we received your material. It's rather thick. I want to assure you that the committee members will have had an opportunity or will have an opportunity to review it. Certainly our researcher will.

We'd appreciate it if you could keep your remarks to roughly ten minutes; then, no doubt, you'll be able to expand as questions come from the members.

Who would like to start? Ms. Lawson.

Mrs. Philippa Lawson (Executive Director, Canadian Internet Policy and Public Interest Clinic): Thank you very much, Mr. Chair, and thank you for the opportunity to testify today.

Good afternoon, members of the committee. In the few minutes I have, I'd like to go over some of the key findings of CIPPIC's two recent studies, which were mailed to each of you last week. I'll then highlight what we think are PIPEDA's major flaws and suggest ways of correcting them.

For more specifics, I would refer you to our written submission dated November 28, 2006. I understand you have an executive summary and the recommendations from that submission with you today. That submission includes a brief description of CIPPIC and of my background, as well as a detailed list and explanation of our 20 recommendations.

I have been working in the privacy field for about 15 years, primarily as a consumer advocate. Since the early nineties, I have worked closely and productively with the Canadian Marketing Association, the Retail Council of Canada, Canadian Bankers Association, ITAC, telecom companies, and other business interests on various privacy-related matters, including the code that forms the basis of PIPEDA.

Since starting up CIPPIC in 2003, I have focused on making privacy laws work by researching marketplace practices, exposing questionable practices, and holding organizations accountable. I've been a staunch advocate of PIPEDA since its conception, and I continue to be a strong supporter of the act.

However, with almost six years of experience with this legislation under our belts, it's become clear that there are a number of gaps and flaws in the regime. I'd like first about what we found when we researched the Canadian data brokerage industry. We found many instances of consumer lists for sale or rent where the likelihood that those consumers had truly consented to the subsequent trading of their names and contact information was highly questionable. For example, one list we found has information about individual and household lifestyles, hobbies, and demographics on almost 900,000 Canadian. The information for this list comes from product registration cards filled out by consumers. Another list has age, gender, home address, and telephone numbers of almost 50,000 frequent travellers in Canada. The information for this was obtained from corporate client databases of airline ticketing offices and travel agencies.

Another list has the gender, monthly income, home and business address of almost 13,000 Canadians with gold cards. This information came from payment processing companies. We found numerous lists offering detailed health information about Canadians who had provided this information on websites or in response to surveys. I could go on and on. This is just a very small selection of the information we found. The point is, there's a vibrant industry in the compilation and trading of these lists for direct marketing and potentially other purposes, and it's not at all clear that the individuals on these lists have consented to such use of their information.

The second study we did is called *Compliance with Canadian Data Protection Laws*. This was conceived and designed for the very purpose of this review. We tested the compliance of 64 online retailers with three of PIPEDA's most basic requirements, those being openness, accountability, and consent. Our sample included large and small companies and covered nine different types of business, from magazine publishers to general retailers. We also tested the compliance of a separate sample of 72 companies with PIPEDA's requirement for individual access.

The results were sobering. In brief, we found widespread non-compliance with the act. Over half of the 64 companies we contacted by phone could not provide contact information for the person in the company responsible for privacy. Two-thirds refused to provide their privacy policy by any means other than their website. Looking a privacy policies, 70% were incomplete in some important respect, 22% were unclear about why they collect the information, 30% were unclear about how they use the information, and 45% were unclear about to whom they disclose the information.

A third of companies we tested don't bother to get consent during the online ordering process. Most companies rely on their privacy policies to get consent. But over half failed to bring the policy to the attention of shoppers, and 60% buried the opt-out consent inconspicuously in their policy.

● (1540)

We found a disturbing number of misleading representations in the policies or on the websites suggesting, for example, that the company would not share your information without consent, but then deep down in the policy it stated that your consent was being assumed. Somewhere between 11% and 39% of our sample required consumers to agree to unnecessary uses and disclosures in order to transact. We couldn't be sure of the number because the policies were unclear.

On individual access—that's the right of someone to access their own personal information held by the company—over a third of the companies to which we sent requests failed to respond at all. Of those that did respond, most failed to answer all three questions we asked. Only 21% fully complied with PIPEDA's requirement to answer these questions.

Our compliance study was conducted in early 2006, five years after PIPEDA came into force. Surely, five years is an ample grace period for companies to get compliant with these pretty basic obligations. So why such a high rate of non-compliance? I think there are two reasons. First and foremost, there's no real incentive for companies to comply with PIPEDA. Second, the act's provisions on notice and consent are unclear.

Something needs to change in the enforcement of this legislation. Companies have to believe that they risk significant reputational or financial damage if they don't comply. That's simply not the case now. Even reckless and wilful violators get away with, at most, a private admonishment from the Privacy Commissioner. We've made a number of recommendations to rectify this situation, most of which do not require any major change to the enforcement regime. Although we think that the commissioner should have order-making powers, there are a number of other amendments that could collectively create the kinds of incentives that industry needs. I refer you specifically to recommendations 3 to 11 in our written submission.

Another possible reason for some of the non-compliance we found is that certain of the act's obligations are unclear. Notice and consent requirements, in particular, are poorly drafted. Now, I take some responsibility for that. I was on the CSA committee, but the CSA code was drafted as a voluntary code, not as legislation. I think I can safely say that no one on the committee ever expected that it would become law as drafted. Alberta and British Columbia have done a much better job of articulating the obligations that PIPEDA meant to convey. We therefore recommend a redrafting of PIPEDA's consent provisions along the lines of the Alberta legislation.

Our study also exposed strange gaps in the act that limit its effectiveness. For example, there's no clear requirement to advise people as to how their information will be used. That's just implicit in the consent requirement. Second, there's no requirement for organizations to disclose the source from which they got your information if you ask them. And there are no special limitations regarding the collection of information from children, whose credulity and ignorance can easily be exploited by commercial interests.

We've provided you with recommendations addressing all these gaps and drafting issues. I don't have time to cover the rest of our recommendations, but let me briefly mention data breach notification.

Over the past year, CIPPIC has been leading a multi-researcher project on identity theft, funded in part by the banks. Identity theft strikes relatively few unlucky individuals, but when it strikes, it can be devastating, and its incidence seems to be growing. There's nothing in PIPEDA that requires organizations to inform affected individuals of security breaches that make them vulnerable to identity theft, and there's little market incentive for organizations to expose their faults voluntarily. We think there should be a legislative requirement for organizations to notify individuals when their data is exposed to potential abuse. We've been researching the existing Canadian law on data breach notification, the various approaches being taken in the United States to this issue, and the arguments for and against. We will be publishing a white paper on the issue with detailed recommendations before Christmas, and I would be happy to share that with you.

● (1545)

Thank you very much for your time. I'd be pleased to answer any questions.

The Chair: Thank you very much, Ms. Lawson. And may I thank you on behalf of the committee for your submission, your executive summary, which was very helpful, and the very comprehensive set of recommendations that you've put forward. It's very much appreciated. That's number one.

Number two, even though I said I wouldn't, I introduced virtually everybody up there. But given the fact that many years ago I used to be an articling student, I want to acknowledge at the front of the table the presence of Ms. Amanda Tait, articling student for the Public Interest Advocacy Centre.

And I think I introduced you, didn't I, Mr. Stark? So I think I've gotten everybody, even though I said I wouldn't. So welcome.

Mr. Lawford, it's up to you now.

Mr. John Lawford (Counsel, Public Interest Advocacy Centre): Thank you very much, members of the committee. Thank you for the opportunity to speak today.

The Public Interest Advocacy Centre has been deeply involved with the Personal Information Protection and Electronic Documents Act, PIPEDA, from a consumer perspective from before its passage. We're therefore here today to give you the consumer perspective on PIPEDA so far.

First of all, PIPEDA is not working for consumers. PIPEDA is, to quote Professor Michael Geist, a "placebo privacy protection". Canadian consumers think their personal information is being protected by a dedicated consumer privacy act, but in practice it is not. We therefore have three requests of this committee. First, the commissioner should be handed order-making power. Second, consumers should be notified when their personal information that is held by a business is lost or stolen. Third, the consent sections of PIPEDA should be clarified to ensure that real informed consent of consumers is obtained when they offer up their personal information.

I'll deal first with order-making power. PIAC completed a study on the consumer experience under PIPEDA in 2004. It found a number of problems for complainants, including the lack of enforcement, above all, by the Privacy Commissioner, in order to vindicate them when they had a successful complaint. Other problems were the frustration of complainants that the commissioner did not, as a matter of course, name the company that had not followed the act, and that the reasons given by the commissioner for their findings were so brief and sanitized that no one else could benefit from their experience in bringing their complaint.

Secondary marketing purposes for personal information gathered from consumers now are so important to business that there is no incentive for them to change practices. Only order-making power of the commissioner will act as a counterbalance to the trade in personal information. Still, the Privacy Commissioner has come before you and said that she does not want order-making power. She said it would decrease the office's overall efficiency and they would be using other powers to get results. We disagree. We think that order-making power would increase the efficiency of the mediation and other processes of the office, as it would act as a stick to the carrot of mediation. As noted in our report, many companies simply ignore the office's findings. The commissioner cannot threaten to take every finding to the Federal Court. Provincial privacy commissioners, however, get results because they have this power to make orders backing up their mediation efforts.

If the OPC—that's the Office of the Privacy Commissioner—intends to perform more audits, for example, order-making power is a natural complement to the audit power. However, at present if there is an audit that discovers practices that are not in compliance with the act, the commissioner has no power to order those practices to be changed. If we add this to the requirement to have reasonable grounds on the audit power, then the commissioner's promise to police PIPEDA with more audit powers looks very suspect. As noted by CIPPIC, there is a widespread non-compliance by business with the most basic and fundamental provisions of PIPEDA, those that are intended to provide the consumer privacy in the marketplace. We therefore do not see order-making power as a luxury, but rather as a necessity.

I'd like to deal now with the issue of naming names in particular. We also think that the Office of the Privacy Commissioner is being far too reluctant to use the powers of her office that she does have. Chief amongst these is the power to make any information gathered in her inquiries under the act public, if it is in the public interest. And this is subsection 20(2). The commissioner has effectively indicated that she will never use it. Maybe, just maybe, she will for repeat offenders. But we've never seen it used this way, and we believe the Canadian Marketing Association has nothing to worry about in this regard.

However, if consumers are to have any effect on the bad actors in the industry on the subject of privacy, they must be able to express their displeasure to the company involved. This cannot be done when the company is protected from any adverse publicity or consumer action. If this committee does not recommend full order-making power for the commission, then at the least we are calling for you to ask that the present section 20 of PIPEDA be reviewed and amended to direct the publication of names of respondents.

I'll turn now to the concept of breach notification. Our second main point is that for a data breach, companies should be required to notify customers under PIPEDA. This would be real protection for real people. Identity theft is either the goal of, or the likely consequences of, many lost and stolen corporate databases of individuals' personal information. Remember that it is real people whose real personal information is lost by companies, and that those individuals will either suffer real financial loss due to the identity theft, or will have to take measures to guard against it, and even if no harm results they will be worried about it.

● (1550)

Covering up the truth, however, will do nothing to help people with this situation. They must be informed in order to make the right decisions for themselves about how to deal with identity theft.

This is the heart of our support for the breach notification requirement. We feel that companies hold personal information in trust and that they must make every effort to protect the beneficiaries of that trust—consumers, customers—by being as open as possible and admitting to losses of personal information.

Canada is not leading in this very practical aspect of privacy protection. Several U.S. states, including notably California, have passed very comprehensive breach notification acts even without underlying privacy legislation. We note also that the Ontario law in the health area requires physicians with a data breach to notify their patients. Other provinces may be considering such breach notification.

We do not think Parliament should take a "wait and see" approach to breach notification, because this places the risk of identity theft on the consumer and not on the company, which, as I noted, should be considered to be in a position of trust.

Consent is our last issue. First, the main point to remember about PIPEDA is that it requires individual consent to all collections, uses, and disclosures of personal information, with only some very limited exceptions. This is the guiding principle and main point of the act, giving people a right of say over their personal information held by others.

Consent was looked at by the courts in a case arising out of a dispute over phone company listings. In that case, Englander v. Telus, the Federal Court of Appeal said clearly that what consent means under PIPEDA is informed consent; that the individual must clearly know about the proposed collection, use, and disclosure of their personal information and agree to it.

This concern applies directly to the argument over what should be standard business practice for obtaining consent to direct marketing or secondary marketing. It suggests that PIPEDA should be amended to define levels of consent, and that the highest possible level of consent—the one tending towards true, informed consent—should usually be required.

In practical terms, this means that opt-in consent should be the default, and opt-out consent only when the company ensures that the consumer is fully informed of what will happen to their personal information.

We're concerned with the CIPPIC reports and believe they demonstrate that the majority of retailers are not likely meeting this standard for consent, and that it is imperfectly expressed in PIPEDA. We therefore urge the committee to adopt the technical amendments to the consent sections of the act that are outlined in CIPPIC's written submission and are designed to clarify this concept so that retailers and other heavy information users can rely on true customer consent.

In summary, PIAC therefore can say that we are asking that this committee give consideration to granting order-making powers to the Privacy Commissioner; that a data breach notification requirement be added to the act; and that clearer rules on consent, in line with those suggested by CIPPIC, be added to the act.

Thank you very much. I welcome any questions in either language at the close.

● (1555)

The Chair: Thank you very much, Mr. Lawford.

Again, we appreciate your very extensive brief and the recommendations you made, which start on page 22, for the interest and information of members.

Now we go to the Marketing Research and Intelligence Association. I think it's Mr. Brendan Wycks who's going to make the presentation.

Go ahead, sir.

Mr. Brendan Wycks (Executive Director, Marketing Research and Intelligence Association): Thank you, Mr. Chairman.

Good afternoon, ladies and gentlemen. My name is Brendan Wycks, and I'm executive director of MRIA, the Marketing Research and Intelligence Association.

Allow me to briefly introduce the other representatives of our association here today. David Stark is chair of our association's standards committee. David is a vice-president and privacy officer for North America at TNS, a corporate research agency member of our association, based in Toronto. Also with us is Alain Choinière, chair of our government relations committee and president of corporate research agency member, CRA/COGEM, based in Montreal; and Mr. Greg Jodouin, our government relations consultant. Mr. Choinière and Mr. Jodouin are available to assist us in answering questions that may arise following our presentation.

We thank the members of the access to information, privacy, and ethics standing committee for allowing us to present our views to you today on the Personal Information Protection and Electronic Documents Act. Let me begin by stating that we are very supportive of PIPEDA and have been since its inception, having been involved as early as the mid-1990s, during the drafting of the Canadian Standards Association's voluntary privacy code that eventually made its way into the PIPEDA statute.

MRIA is the single authoritative voice of the market and survey research industry in Canada, representing all of its sectors. Our members include over 1,800 individual research professionals and more than 260 corporate members. Those are comprised of research agencies of all sizes and specializations, from sole proprietorships such as focus group moderators, to large global full-service agencies and, in addition, many buyers and users of research services, such as the major Canadian banks and other financial services industry players, national retailers, insurance companies, telecommunications firms, and manufacturers.

It perhaps goes without saying, but one of the major pillars of the market and survey research industry is the good relationship that exists between researchers and the general public. We devote a significant amount of time and effort to protecting that relationship through our long-standing self-regulation of our industry, much of which centres around protecting consumers' right to privacy. As another example, legitimate researchers are forbidden from trying to sell anything. That's one of the key principles that are front and centre in our rigorous standards of practice, and it is now enshrined in our recently released charter of respondent rights.

It's an absolute necessity to the ongoing viability of our industry that we protect that healthy relationship with Canadians and the reservoir of goodwill that exists for survey researchers. In that vein, we also have a long history of working closely with the federal government on policy initiatives that enhance consumer and privacy rights in Canada. An important fact that you may not be aware of is that the federal government is the single largest user of survey research in Canada. As a major research user, the government indirectly benefits from the impact that our self-regulatory initiatives have in strengthening consumer rights and improving accountability.

All told, MRIA and the industry we represent are advocates and champions of an enhanced privacy framework in Canada. We are happy to be here today to make some suggestions on how Parliament can achieve a stronger, more effective national privacy regime. We applaud the government's and the Privacy Commissioner's ongoing efforts to enhance privacy and consumer rights.

Turning now to the act itself, we believe PIPEDA has proven to be effective legislation that has brought about considerable change in the way businesses operate. No doubt, it has resulted in a collective raising of the bar, across the board and for all industries, in how personal information is collected, used, and disclosed. But as with all new initiatives, the wrinkles only appear when they are put to the test, and the past six years have shown us what works well and what could be improved.

We' d now like to make a few recommendations on how to strengthen PIPEDA.

First, we believe the law should be amended to require organizations to disclose to individuals breaches of their unencrypted sensitive personal information. The majority of U.S. states already have such security breach notification laws in force. It's paradoxical that PIPEDA requires organizations to use physical, technological, and organizational safeguards to protect the personal information that they collect, but that currently there is no explicit requirement to notify individuals when their sensitive unencrypted personal data are compromised, such as one's name in combination with any of the following: social insurance number, driver's licence, credit card number or bank account number with accompanying security code, passport number, or other information that could be used by criminals to propagate identity theft.

Market and survey research firms do not collect from consumers the types of personal information that I've just mentioned. Our industry suffers, however, when online identity theft occurs, because that fraudulent criminal activity makes Canadians less trusting of reputable businesses and less willing to disclose their personal information for bona fide, legitimate purposes.

● (1600)

Second, we would like to see PIPEDA amended to give the Privacy Commissioner order-making powers. The commissioner should be empowered to issue binding findings, including the levying of fines and the imposing of penalties or mandatory reporting requirements on organizations that demonstrate a blatant disregard for Canadians' privacy rights. Privacy abusers should not be able to enjoy the benefit of anonymity in case summaries appearing on the Privacy Commissioner's website. If the Privacy Commissioner were able to identify organizations that have been the subject of well-founded complaints, they would surely improve their personal information management practices to avoid becoming the focus of media attention and suffering damage to their corporate reputations.

Third, we also believe PIPEDA should be amended to allow the transfer of personal information from an organization to a prospective purchaser or business partner. As part of this, organizations should address mergers and sales in their privacy policies, to permit the transfer of individuals' personal information. For its part, the receiving party should be required to honour the terms and conditions in the transferring party's privacy policy. If the acquiring party wishes to amend the privacy policy, then it should provide an option for individuals to opt out of any material changes to the collection, use, and disclosure of their personal information.

Finally, we would like to comment on a serious industry issue as it relates to PIPEDA and why we would like to see tougher enforcement of the law. We call this issue “mugging and sugging”, or marketing under the guise of research and selling under the guise of research.

In recent years, a number of pressures have begun to encroach on the reservoir of goodwill that Canadians have historically shown toward survey research. The explosion of direct selling and telemarketing activities over the past decade has also added to the sensitivity Canadians have about participating in survey research. Some unscrupulous direct marketers and fundraisers who use the guise of survey research in their sales pitches have exacerbated this situation.

As disciplined as researchers are in respecting consumers' privacy rights, the actions of other industries can damage the relationship that exists between researchers and the general public. This has been an ongoing concern for MRIA, notably with the increasing prevalence of mugging and sugging practices.

Just to give you a bit of backup information about this, MRIA periodically conducts a survey on Canadians' attitudes towards survey research, as a form of pulse check on our industry and respondent privacy protection. Our most recent fielding of this survey, conducted in late 2004, shows that the generally positive attitudes toward survey research continue to be fuelled by a recognition among Canadians that survey research serves a valuable purpose in society, because it allows them to give voice to their opinions and to have input into and influence decisions about public policies and about products and services in the marketplace.

In our 2004 survey, 87% of respondents agreed that research surveys give people the opportunity to provide valuable input and feedback. That was up three percentage points over the responses to that same question when we conducted the survey in 2001. In terms of those who agreed that the survey industry serves a useful purpose, 78% agreed, up slightly from 2001. Of particular interest to parliamentarians, 73% agreed that research surveys and polls are useful for government to understand how the public feels about issues.

The 2004 study results, however, underscore the persistent serious threat to our industry posed by mugging and sugging. Mugging and sugging, marketing and selling under the guise of research, occur when direct sellers and fundraisers pretend to conduct a research survey to gain the confidence of a potential target. There is no doubt that this illegal activity has an adverse effect on the positive attitude that the general public has toward participating in research surveys. More than half, or 53%, of respondents in our 2004 survey had been contacted in the previous year for an alleged research survey that actually turned out to be an attempt to sell a product or service. More than one in four, or 27%, of respondents in our 2004 survey had been contacted in the previous year for an alleged survey that actually turned out to be an attempt to solicit money for a charity or for some other cause.

As things currently stand, PIPEDA makes it illegal to mug and sug. The identifying purposes for which muggers and suggers seek and obtain Canadians' consent are fraudulent. Consent is obtained under the false pretenses of survey research, and the collected personal information is used for other than the stated purposes—not for a legitimate survey, but for sales. Yet our research shows that these unscrupulous practices still occur. Occurrences of mugging and sugging were at the same level in 2004 as our previous survey had found in 2001. Mugging and sugging had not diminished at all.

● (1605)

And now, with the coming implementation of the national “do not call” registry in 2007, unscrupulous telemarketers will have another incentive to flout the law by practising mugging and sugging. And that would erode the public goodwill that legitimate survey researchers have earned.

We therefore urge the Government of Canada to amend PIPEDA to give the Privacy Commissioner order-making powers so that, together, we can put the muggers and suggers out of business and protect Canadians from their scams.

To wrap up, market and survey research plays a pivotal role in our society by giving voice to the opinions of Canadians and helping to influence and improve public policy decisions. There are two key characteristics that define market and survey research and differentiate our work from that of the telemarketing industry. First, legitimate survey researchers never attempt to sell anything. In fact, solicitation violates our rigorous code of conduct and ethical practices.

Second, survey research gives Canadians an opportunity to voice their opinions and to have influence on important issues related to public policy and products and services, thereby serving a valuable societal purpose. For these reasons, it is critical that the right legislative framework exist in Canada, to protect the essential work that survey researchers do. PIPEDA went a long way to achieving that. Yet, the six years since its adoption have demonstrated that the legislation must go further still. MRIA and the survey research industry believe that important amendments must be made to PIPEDA that will make the legislation more effective in protecting Canadians' privacy rights.

To summarize, our PIPEDA amendment recommendations are as follows. First, organizations should have to disclose to individuals any breach of their unencrypted sensitive personal information. Second, under specified conditions that protect privacy rights, PIPEDA should allow for the transfer of personal information from one organization to a prospective purchaser or business partner. Third, the Privacy Commissioner should have order-making powers, such as the power to making binding findings or to impose fines or other penalties. Finally, and most important to the market and survey research industry, those order-making powers should provide the Privacy Commissioner with the necessary tools, resources, and jurisdiction to enforce PIPEDA and to once and for all put an end to fraudulent mugging and sugging practices.

MRIA appreciates this opportunity to present the views of the market and survey research industry as part of this important legislative review. We'd be pleased to provide further comments as your proceedings evolve and as information on potential amendments to PIPEDA is released.

Thank you.

The Chair: Thank you, Mr. Wycks.

Could I get a clarification? Your statement that mugging and sugging is illegal under PIPEDA, is that because of the lack of informed consent? Is that what you're talking about? Or is there a specific section that deals with that?

Mr. David Stark (MRIA Standards Chair, Marketing Research and Intelligence Association): One of the principles is that organizations must identify the purposes, the reasons why they are seeking to collect personal information. So when muggers claim to be doing a survey, when that's the identified purpose that's disclosed, they're not in fact genuine about what they're doing. They're calling people to try to sell them something, and that's not disclosed until after Canadians have given information, ostensibly for the purpose of a survey. That goes against the identifying purposes, the principle, the fact that the purposes must be disclosed before or at the time of collection. Since the sales pitch is not disclosed until the very end, then the way they use that information also goes against PIPEDA.

But there's another statute, amendments to the Competition Act that were made, I think, about seven years ago. Those amendments require telemarketers to disclose within the first 30 seconds of their call their name, the name of the organization on whose behalf they're calling, and the purpose of their call. So they really can't be using fancy footwork, like mugging and sugging, to hide what their true tactics are, if their purpose is to try to sell something.

So there's a couple of statutes where it's illegal: the amendments to the Competition Act and some of the principles within PIPEDA. Obviously, through order-making powers and better enforcement, I think we could go a long way toward putting an end to mugging.

● (1610)

The Chair: Thank you very much.

We have our first round at seven minutes for each questioner, including answers.

We'll start with Mr. Peterson.

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

I join with the chair in commending CIPPIC and PIAC for the wonderful briefs you've presented to us and the research you've done.

I ask you, Mr. Wycks, how do you feel about blanket consents? Do your members use them, in terms of using personal information?

Mr. Brendan Wycks: Generally when researchers call Canadians, if it's a survey by phone, or if it's inviting Canadians to join a panel to—

Hon. Jim Peterson: Do you get consent to pass this information on?

Mr. David Stark: We obtain consent to conduct the survey, or when we invite people to a focus group, they agree that they will participate or not. It is an opt-in consent. We don't pass on information for secondary purposes, because we don't try to market products or services.

Hon. Jim Peterson: You said you can sell the data, including personal information.

Mr. David Stark: No, that—

Hon. Jim Peterson: Was that not one of your recommendations? I misunderstood you, then.

Mr. David Stark: No, not at all.

Hon. Jim Peterson: What was your second recommendation?

Mr. David Stark: The recommendation is that if a prospective purchaser of a research firm, or any business, wants to buy another, and that business has customer records or personal information in place, then whenever a business transfer occurs, the legislation should be clear in stating what is and is not permitted—

Hon. Jim Peterson: Oh, that's all. You're talking about selling a business that has data, and not the data itself.

Mr. Brendan Wycks: That's right.

Hon. Jim Peterson: Okay, you don't believe in opt-out consents.

Mr. David Stark: No.

Hon. Jim Peterson: And you don't believe in blanket consents. None of your members would use them.

Mr. David Stark: No.

Hon. Jim Peterson: Could I ask you, Mr. Lawford and Ms. Lawson, is there any room between you on any of these issues or are you *ad idem* totally?

Mr. John Lawford: I believe we're almost identical in our viewpoints.

Hon. Jim Peterson: I certainly felt that way.

Let me go to the order-making power. You've shown that there are at least three other powers that could be used more effectively: corporate audits, the initiation of complaints, and naming. If those were being fully used, would you want order-making power in the hands of the Privacy Commissioner?

Mr. John Lawford: Speaking for PIAC, I'd say we would still like to have order-making power, because of companies in the past that have demonstrated they will not follow the findings of the Privacy Commissioner—repeat offenders.

Hon. Jim Peterson: How many people have been named by the Privacy Commissioner for breaches so far?

Mr. John Lawford: We were having this debate earlier. We think it's either one or zero.

There was an Air Canada dispute over the flight points program, and Air Canada's name came out. I don't recall another situation where the Privacy Commissioner has ever named anyone.

Hon. Jim Peterson: How many cases have gone to court so far?

Mr. John Lawford: We believe there are at least 350 findings.

Mrs. Philippa Lawson: Very few have gone to court. Most of those that have were settled.

Hon. Jim Peterson: The Privacy Commissioner was very adamant that she not be given this order-making power until she has been given a chance to try these alternative remedies.

Mrs. Philippa Lawson: I have a bit of difficulty with that. First of all, she and previous commissioners have had a lot of time to use these other powers.

We also have some concern that some of the messages we've been getting from the Privacy Commissioner's office suggest that there is an interpretation of the law that doesn't allow them to name names. That's why one of our recommendations, and PIAC's too, is to clarify that, so it is clear that not only is she allowed to name names, but in fact she must in certain cases.

Like PIAC, we at CIPPIC feel that the order-making power would complement all these other powers and would help to make the legislation more effective.

Hon. Jim Peterson: Can you compare the practice of the three provinces with what's happened federally? Is it more effective?

Mrs. Philippa Lawson: That's a very good question. I was asking myself that. We didn't study that. It's very hard to do. I was trying to think of how I would construct a study to try to measure the effectiveness of the legislation, for example, business compliance. I suppose what we could try to do in a future study would be to pick some companies that are regulated under the Alberta legislation, and some under B.C. and Quebec, and compare federally. You'd need a pretty big sample to come up with a significant result.

● (1615)

Hon. Jim Peterson: A lot of your recommendations are excellent, particularly in the consent area. We can learn a lot from you there.

On data breach notification, your study points out that in less than a year—since last February—50 million Americans have been compromised in terms of their personal information. Would you like to expand on the types of notice you think we should make available to those who have been compromised?

Mrs. Philippa Lawson: You're asking for specifics on how the notice should be delivered or on what should be in the notice.

Hon. Jim Peterson: Yes. I noticed that you said you're not calling for registered letters or phone calls to everybody. You're just calling for e-mails or general—

Mrs. Philippa Lawson: Yes, our recommendation—and I'll let the others speak to this too—is that notification should generally be by mail, but electronic and substitute notice should be permitted, as appropriate. I think there should be some flexibility there for organizations, but we do think this is a business cost that is worth incurring and that it will have the effect of an incentive for businesses.

Hon. Jim Peterson: Do you think it should be by registered mail, so we're certain that it has been delivered?

Mrs. Philippa Lawson: That's a good question. We haven't proposed registered mail specifically, but it's something to think about.

Mr. John Lawford: The difficulty would be with very large losses, of course. The California legislation allows for substitute notice through a newspaper of general circulation for really large ones—

Hon. Jim Peterson: Which might not be very good at all.

Mr. John Lawford: It might not be very good at all, but it might be the only way to do it if there are half a million.

Hon. Jim Peterson: Would you consider a notice provision that would have to be worked out with the Office of the Privacy Commissioner in every case?

Mr. John Lawford: I'll just speak from PIAC's point of view.

We support having the Privacy Commissioner apprised as soon as possible of a data breach and having the Privacy Commissioner give advice to the company involved, but we do not support the Privacy Commissioner having discretion to make a call on whether notification should be given or not given. They're reluctant so far to do things—

Hon. Jim Peterson: But your recommendation....

Thank you.

The Chair: I congratulate you. You must have gotten 10 questions in there in seven minutes, and the answers.

We'll go to Monsieur Laforest.

[*Translation*]

Mr. Jean-Yves Laforest (Saint-Maurice—Champlain, BQ): Good afternoon to you all.

Since the beginning of the hearings, some subjects have come up often, including consent and the power to make orders.

With respect to the power to make orders, Ms. Lawson said earlier that the Alberta Act could serve as a model. When he was asked, the commissioner replied that it worked well in Alberta and British Columbia, but that it wasn't necessary to add an order-making power for the commissioner in the federal act. And yet a number of witnesses have told us that would be important, because it would toughen up the legislation and give the person enforcing it more power.

So we're hearing two contradictory versions. Your group's version leans a bit more toward grassroots public interest. How can you help us sort this out?

● (1620)

Mr. John Lawford: To begin with, in our experience, there have been organizations that didn't really follow the commissioner's recommendations. In those cases, particularly if the name of the organization is unknown, consumers will want to solve the problem themselves, by no longer dealing with the company or whomever.

I should also point out that in the provinces, for example, in British Columbia, an order is not made every time. The power is there to persuade companies that are a bit reticent to change their practices. I think it works well.

Mr. Jean-Yves Laforest: It's more effective.

Mr. John Lawford: Yes.

Mr. Jean-Yves Laforest: Does anyone have anything else to say?

[*English*]

Mrs. Philippa Lawson: Yes.

I would add that we have trouble understanding why there is so much reluctance to adopt an order-making power at the federal level when it seems to be working very well in all three provinces, Quebec included, not just British Columbia and Alberta.

The reason we've pointed to the British Columbia and Alberta models is that they were modeled on PIPEDA three years afterwards. They got the advantage of seeing how the federal legislation was working and improving on it in a way that Quebec didn't, because Quebec was the first one out of the gate.

I have trouble understanding the opposition to order-making powers, because I think it's clearly proven to be a complementary tool in the hands of the provincial privacy commissioners.

[*Translation*]

Mr. Jean-Yves Laforest: With respect to consenting to the disclosure of personal information, one witness told us that it wasn't necessarily a problem of knowledge,but that it was more an issue of... It's as if the information or the rules weren't clear. I would say it's more a matter of making the rules better understood.

Do you agree with that, that it's more a matter of overall understanding than knowledge? Have you raised the problem of the need for more explicit consent?

[*English*]

Mrs. Philippa Lawson: I have a question of clarification. Are you asking about the businesses' understanding of their obligations under the act or about the consumers' understanding of the businesses' practices?

[*Translation*]

Mr. Jean-Yves Laforest: I'm talking about consumers.

Mrs. Philippa Lawson: You're talking about consumers.

[*English*]

I would agree with what John stated, that the intention of this legislation is to ensure informed consent, which means the knowledge, the full knowledge of individuals about what the business is doing with their personal information. That is not stated clearly enough either in the legislation, speaking to the organizations, or in the organizations' privacy policies to consumers, in many cases. Businesses need to do a much better job conveying that to individuals, and the act needs to communicate better to the organizations.

[*Translation*]

Mr. Jean-Yves Laforest: It's a bit like using overly legalistic language to inform consumers. It's not that they're lacking information; it's that the information is hard to understand.

[*English*]

Mrs. Philippa Lawson: Yes.

We did scientific readability tests on the 61, I think it was, privacy policies we had overall. They all measured way above average. The average was way above average. I don't have it before me now, but on the scales we measured it, we did eight or ten different readability tests, and they were all above grade 13 comprehension levels, well above the standard English level.

Often these corporations are not communicating in plain language to individuals. The act requires them to do that. The act says it has to be generally understandable, it has to be reasonably easy for individuals to understand what's happening with their personal information. We had law students testing this, and they found—I gave you the percentages—in a large minority of cases what was going on was not clear to a law student.

● (1625)

[*Translation*]

The Chair: I'm sorry, time is up.

[*English*]

Perhaps our witnesses could ponder the following, and then we'll go to Mr. Tilson.

Each of you has recommended order-making powers. The British Columbia commissioner was here, said he had his order-making powers, said he rarely if ever uses them, and—as I understood the evidence—supports the current Privacy Commissioner's lack of a call for order-making powers. The current Privacy Commissioner was the Privacy Commissioner for the Province of Quebec and had order-making powers when she was the commissioner for Quebec and now doesn't want them. I find that curious, given your unanimous recommendations.

I'm not asking for an answer, I'm asking you to ponder that while we go to other questions.

Mr. Tilson.

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

I'd like to ask a question I've asked most of the witnesses who have come before us, and that has to do with small businesses. I've asked whether or not, with PIPEDA, small businesses are adequately looked after. In my community I'm thinking specifically of one business, a drycleaning business, but it could be a small mail order business in someone's home. There could be one or two individuals involved. We have a lot of those in our area. Almost all of you are talking about the contact with the corporation, or the privacy person with the corporation. For these people I'm referring to, there's no way in a million years they can afford to do all that stuff. Do they even have the resources to respond to some of the issues you're talking about or, indeed, what PIPEDA requires?

My question is getting a little long. I started off by saying to groups and, in fact, to the commissioner, are small businesses being looked after? Almost to a T, the answers have been “No, we could do a lot more”, or some vague answers such as that.

I wonder if all three groups could comment on that issue.

Mrs. Philippa Lawson: Thank you.

It's a good question. I think certainly more could be done in terms of educating small businesses and getting the word out about what they have to do under PIPEDA. I think there may be a perception out there that it's much more onerous than it actually is. PIPEDA does not require every organization to have a separate privacy officer. If it's a sole proprietorship, a small business, the guy in charge of privacy is the guy running the business.

Mr. David Tilson: Mr. Chairman, I appreciate that, except that you're all talking about the issue of consent, or disclosing violations of the legislation. They won't know what in the world you're talking about.

Mrs. Philippa Lawson: And it probably won't ever affect them. This is largely directed toward businesses that are in the business of dealing with personal information.

Mr. David Tilson: I challenge you on that. If it's the one-person retailer who gets credit card information, they all say, "Oh, could I have your telephone number too, please?" or "Could I have your postal code?" And they all do that. Where does that information go? We all know where it goes.

Mrs. Philippa Lawson: This is the question. Why are they asking for that information? Do they really need to? If once they're getting into that business—

Mr. David Tilson: That's why I'm asking this question. You say PIPEDA isn't going to affect these people. Well, listening to your own answer, I think it is going to affect these people.

Mr. John Lawford: May I answer?

To the extent that it does affect the smaller businesses, we simply think it's good business, because if a customer finds out after the fact that there has been a loss of their personal data and it led to identity theft, that business would feel terrible and they would lose business in the long run. We think that it's good to get the issue in front of them—as Philippa said, an incentive—to have them take even a very general look at their data-handling practices, if you will, and put things under lock and key. They may think about maybe running a really simple encryption program. Even knowing what kind of information they have, it's not that onerous.

Mr. David Tilson: You know, sir, I understand what you're saying. But I go into my local drycleaner and I can still remember his talking about PIPEDA. He said this thing was killing him. He does know, people do know about certain requirements that the federal government has.

I don't want to spend a lot of time; I'm simply trying to make a general observation about how we are all talking about the big companies or big telemarketers, or whoever, but we're not talking about the little guy, and that's what I'm trying to get out of all witnesses. What recommendations do you have to inform the little guy? And also, little guys can break the law too.

Mr. David Stark: I share your frustration. Let's face it, the small convenience store operator won't necessarily have a written privacy policy that's posted, and all of these things that are required under the statute. Where I hope some organizations might attempt to assist the small business owner would be the various trade associations.

I don't know what the Canadian Federation of Independent Business has done for their members, but our industry association produced a privacy protection handbook. And recall that our association represents not only large corporate members but sole proprietors, focus group moderators, small business people. They have a comprehensive set of tools through their industry association that will help make it much easier for them to comply without incurring significant legal costs. I'd like to think that many other Canadian trade associations are helping their small business members to some degree.

● (1630)

Mr. David Tilson: Most Canadians, I believe, haven't the slightest idea of what their privacy rights are. I believe that. I've listened to witnesses, and many witnesses have agreed to the same thing. The Privacy Commissioner has said—and it's an interesting philosophy—that we need to educate. We need to spend more time educating the general public as to what their rights are.

The Privacy Commissioner's budget is over $16 million. It's a lot of nickels. My question is, who should do that education? Should it be the government, the Privacy Commissioner, or should it be businesses?

Mr. John Lawford: I believe the Privacy Commissioner has the mandate, under the act, to do some public education, and we do acknowledge that they have some guidelines on their website. I'm not sure of their plan for reaching out in the future. I believe it was referred to in the last report that they were going to put something more in place. I believe we can count on them for some of that, but I do like the suggestion that there may be alternate routes to getting the message out there. Certainly from consumer organizations' point of view, we're happy to work with the business organizations to do that.

Mr. David Tilson: So you think it should be a combination of both, that both the business organizations and the commissioner should participate. How would business organizations do that?

Mr. John Lawford: I'm just going to take a stab in the dark here, but I know the Privacy Commissioner does meet with the business organizations on a fairly regular basis, and this is something that certainly could come up in discussions with them at that time. We would be happy to participate, as well, to the extent that would exist.

The Chair: Thank you, Mr. Tilson.

We start our five-minute rounds, and I'll start off.

Ms. Lawson, you said the act has been around five years, so why hasn't everybody complied? We heard, I believe, that in fact it's only been around fully for about two years—January 1, 2004, isn't that right?—so why do you say five, and I think you gentlemen said six?

Mrs. Philippa Lawson: It's six years.

The act came into force on January 1, 2001, and everyone knew about it then. The provincially regulated businesses were given three years' grace period, basically, before it became effective for them. So they had that first three years to think about it and get educated and get ready for it, and then it's been an additional two years since then that they've been under the legislation, subject to the legislation. So there's a distinction for some businesses between just the legislation being there but their not being subject to it, and their being subject to it.

The Chair: I believe it was the Canadian Marketing Association that said that for them it came into force on January 1, 2004. I think that's what they said.

Mrs. Philippa Lawson: That's not true. For many of the members of the Canadian Marketing Association, it's been effective since 2001. For some of their members it's only been effective since January 1, 2004, but it's been around since 2001, and they all knew about it.

● (1635)

The Chair: Okay.

Mr. Lawford, you said the respondents' names should be published.

Mr. John Lawford: Yes.

The Chair: What about requesters whose requests have been deemed to be frivolous or who have asked for information for what is determined by the Privacy Commissioner not to be a valid reason, validly requested, and it costs the company a lot of money? Should their names be published?

Mr. John Lawford: No, we don't think so.

The Chair: Why?

Mr. John Lawford: Because privacy is personal to the individual, and that further publication of their name will, in their view, also victimize them from a privacy point of view. It's special that way, and we do acknowledge that is a special situation, because we're dealing with personal privacy.

The Chair: Even if the requests were frivolous and vexatious?

Mr. John Lawford: Even if their requests were frivolous and vexatious, because we don't think there are a lot of those complaints, and that in situations like that—

The Chair: That may be.

Mr. John Lawford: —there are still routes for the company in the court system, if they feel they are being attacked in an unfair way, to try to address that.

The Chair: Okay.

On this naming names, if you feel that a particular—and not this one, but a particular—Privacy Commissioner is reluctant to use what they already have, section 20, etc., what makes you think they'll be any less reluctant to use order-making powers?

Mr. John Lawford: That's a fine question. If there's an organization that is being investigated further than just mediation, if it's a resistant organization, let's say, I'm sure the Privacy Commissioner will come across situations where they get no response from the company, where they have had an egregious situation, and in those cases the Privacy Commissioner will want to get an order out there. For repeat offences, I think at that point the Privacy Commissioner will see the value in laying down the law, if I can put it that way, to someone who has ignored the last two findings. Those will be the situations where it will start to happen.

The Chair: Finally, if there's only been zero to one name named, how does one know whether or not businesses are ignoring the Privacy Commissioner?

Mr. John Lawford: We have determined, through very careful reading of the rather cryptic findings—a number of examples are in our report—that in at least three cases there are repeat offences for the same bank, because the commissioner at the time said it was the same bank as in finding number *x*. I can give you the exact numbering if you give me one moment.

The Chair: No, I'm just curious. If it's all so secret, then how do we know that people are specifically going against the Privacy Commissioner?

Mr. John Lawford: There may be more. We found three.

The Chair: But you think it's a bank, or you know it's a bank?

Mr. John Lawford: I have two cases with banks.

The Chair: Okay.

Mrs. Philippa Lawson: There was one case where we made a complaint against the company, and it was the third time. It had been complained about twice before, and you could determine that.

The Chair: I see. All right, thank you very much.

We'll now go to Mr. Wallace.

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

And thank you for coming this afternoon. I have a couple of questions in my five minutes.

I want to ask one directly, right away, and it's on the Canadian Internet policy piece. Your 11th recommendation is to remove the "reasonable grounds" requirement for audits. Does that mean it's unreasonable grounds? What do you mean by that? Being a lawyer, you should be able to answer this question, I guess.

I don't know why you don't think there should be reasonable grounds before we start doing audits.

Mrs. Philippa Lawson: Well, I think it's fine. I think it's a good idea to have reasonable grounds. I think there is a place, however, for spot audits, like randomized spot checks, if the commissioner has the resources to do that, where it doesn't have to be a company against which there have been several complaints. That's one reason.

Another reason is that it seems to be...I mean, the commissioner's being taken to court right now by Equifax for not having reasonable grounds for a particular audit when apparently there were four complaints and a preliminary investigation. It just seems like a tremendous waste of resources to allow that kind of litigation when the Privacy Commissioner is extremely unlikely to engage in that kind of audit without reasonable grounds in any case.

Mr. Mike Wallace: Right. Well, I would agree with you they're likely to have reasonable grounds to go in, and I think in your view or your organization's view, maybe they could do spot audits. Would you not agree, though, that they'll probably require more funds from the taxpayer to make that happen?

● (1640)

Mrs. Philippa Lawson: I'm not sure. The money they're getting right now, $16 million, is a pretty decent amount of money. I don't have the ability to judge what you can do with that.

Mr. Mike Wallace: Okay.

On the consent issue...no, let me go to the naming issue first. I have an issue with naming.

I don't understand why there's an issue, if the commissioner can resolve the problems without the publicity of someone being named. Isn't the whole theory to try to protect people's privacy and not to try to embarrass people because they screwed up?

Mrs. Philippa Lawson: There are a number of complaints that are disputes between one individual and one company, and those absolutely are appropriately dealt with through mediation, resolved and settled, and no one's name needs to be published in those cases necessarily.

But there are many more, certainly the complaints that CIPPIC has lodged with the Privacy Commissioner, that have to do with company policies and practices that are widespread and are affecting thousands and thousands of consumers at once. It's not a question of a dispute that you can mediate. This is a matter where in many cases companies are just blatantly, in our view, violating the law and they think they're right. The issue needs to resolved, and it's an issue that should be resolved publicly, in our view.

Mr. Mike Wallace: Okay, so do you believe their name should be announced prior to their being found guilty—and I use that word loosely—of violating the act?

Mrs. Philippa Lawson: No, I think the release of the corporate name should be after the findings have been made.

Mr. Mike Wallace: Okay. Another question I have for you is on education. We've had some dispute...and I actually agree with a couple of Mr. Wappel's questions. He stole a couple of mine.

On the piece on education, we've heard from some groups that it may have been in place since 2001, in time to get you ready for it, and it took effect in 2004, and so on. But would you agree that the government or the commission has not done a great job in terms of bringing people up to speed on what needs to be done here? I know they've come to see us during budgetary discussions, and some of the new money they're looking for, additional money or whatever it is, is to be geared to education.

I'll be frank. I was involved in municipal council for 13 years, active in business for 20-some years since graduating from university, and since I've been here, it's the first time I've heard of it.

Does anybody want to take a shot at answering that question?

Mr. John Lawford: I have to agree with you that I don't think enough outreach and enough education has been done from a consumer point of view.

Mr. Mike Wallace: So don't you think we're premature in making these major...?

I'll be frank with you. I'm listening to what the commissioner wants to do, first, because they're dealing with it on a daily basis. On the issue, for example, of order-making powers, I'm having a hard time saying, well, this individual who deals with it on a daily basis is saying we need more time with it to see what's happening; and you're using other examples, of course, that are happening. But I need compelling reasons why that person who deals with it on a daily basis isn't giving me the right answer.

Mr. John Lawford: The two aren't incompatible, because you have cases that we found over the last four or five years where some companies are just never going to give in. They will continue the practice. But it's true that a huge amount of education still needs to be done, especially at the consumer end, to say that you have these rights, and at the business end, to say these are your responsibilities and this is how to handle it. I don't see the two as being incompatible.

The Chair: Thank you, Mr. Wallace.

Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): First of all, I'd like to finish up with the question my colleague asked earlier, and then I'll ask my own questions.

Shouldn't the act provide for an explicit consent form?

Mr. John Lawford: At the Public Interest Advocacy Centre, PIAC, we suggested a form that is already in the Quebec legislation. The court decisions are really along the same lines, but it's not explicit.

So we support that kind of amendment.

Mrs. Carole Lavallée: Okay, great. Thank you.

My other question has to do with publishing the names of companies that I would call delinquent. On the one hand, it's clear that the debate is largely focused on the fact that consumers are lacking information on the protection of their personal information. People are always under the impression that they will be protected, or on the contrary, sometimes there are people who are a bit more paranoid and are sure that everyone is distributing their personal information.

On the other hand, when companies are delinquent, their name is not disclosed. Personally, I really have a hard time understanding this fact. I know of no other legislation under which the names of delinquents are not made public, apart from pedophilia cases. I don't understand that.

What's more, you just said the names of delinquent companies shouldn't be disclosed. And yet an organization like yours appears to be interested in defending consumers.

Maybe I missed something. Could you clarify that?

● (1645)

Mr. John Lawford: I think we said exactly the opposite. What we said was that at the very least, the names of delinquent companies should absolutely be published, as well as the names of the people responsible. As for the commissioner's other decisions, the names of companies should also be disclosed, where appropriate.

[*English*]

Mrs. Philippa Lawson: I know that for many years PIAC and also CIPPIC have been calling for the naming of organizations that have been found delinquent under the act.

[*Translation*]

Mrs. Carole Lavallée: How is it that in this legislation, companies have had the privilege of remaining anonymous? Do you know any other legislation like that?

[*English*]

Mrs. Philippa Lawson: The Competition Act is similar.

[*Translation*]

Mrs. Carole Lavallée: The Competition Act.

I am so surprised by that. I'm also surprised to see that other groups, other witnesses have come here... Perhaps we could hear from the people sitting beside you.

Do you think we shouldn't go right ahead and publish the names of delinquent companies?

[*English*]

Mr. David Stark: I think businesses that are flagrant abusers and violators of privacy rights should have their names published. Publishing the names would shame them into compliance, one would hope. They would become media stories, and then that would sort of tie into the question raised previously: how do you increase awareness and consumer education?

If people can be cloaked in anonymity, then yes, of course consumers aren't going to understand their privacy rights and the law. So this is one way of bringing their rights to their attention. Name names. Let's not treat offending organizations with kid gloves.

[*Translation*]

Mr. John Lawford: I'd like to add that we don't interpret the act in the same way as the commissioner does. We feel it is in the public interest to publish those names. It's just a difference of opinion.

Mrs. Carole Lavallée: Mr. Chairman, do I have any time left?

The Chair: You have 10 seconds left.

Mrs. Carole Lavallée: Thank you very much and sorry for being late, it was beyond my control.

[*English*]

The Chair: *Merci*.

Mr. Van Kesteren.

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

Thank you all for coming.

I'm going to follow Mr. Tilson's line. I have to tell you, I get a little nervous. When we spoke to the Privacy Commissioner, my comment at that time was much along the lines of Mr. Tilson's questioning, that we're opening up a whole new bureaucracy.

I'll just give you my example. I was a car dealer before this. I was going to be a lawyer, then I became a car dealer, and now I'm a politician. You can see the regression in my life—at any stage. When this all came about, and when I spoke to my colleagues, we found this a bit terrifying. For instance, I have a staff of sales people. With the documentation we collect, if we sell a car and the other guy says that was his customer, the proof was the documentation. That whole process became an anxiety for a dealership. As Mr. Tilson says, if you're a fairly large dealership you can handle it, but a smaller dealership has to hire somebody.

I'm a little concerned, and maybe we can use the analogy of throwing the baby out with the bathwater. On the one hand, I hear some legitimate concerns, but on the other hand, I'm thinking, my goodness, if somebody wants to....

My wife loves to do the surveys. I can't understand why, but she loves that stuff. She hands these surveys out. She has enough sense when somebody calls, to say no, she doesn't want that. She likes the coupons, I guess, and all that other stuff.

But are we going way overboard for something that's so simple? I mean, for something as simple as notifying the public and saying, listen, I hope you realize that when you give this information you are opening yourself up to such and such, do we have to make new legislation?

I was quite comfortable after speaking to the commissioner that this was not the case, that they weren't zeroing in on small businesses that have no ill intent. But now I'm thinking, good Lord, we're going to get into whole new legislation. That is precisely—and I think I used the term—a reign of terror. Once we get these laws enacted, the government can just start persecuting small businesses. And really, there is no ill intent.

I would just throw that out to you.

● (1650)

The Chair: Let's start with Mr. Lawford.

Mr. John Lawford: If, for example, the smaller businesses are holding personal information and they lose it, I'm assuming they would still be concerned for their customers. That's one of the reasons we brought the one big request here, which is that if they lose it could they please tell people.

Most small businesses are not using the personal information in a lot of secondary ways. They might be doing some mail-outs to their own customers, but they're not in the huge data brokerage industries. We don't see a lot that we're requesting here that's going to impact them any more than the act already does at the moment.

Mr. Dave Van Kesteren: But can't they police themselves? For instance, the insurance industry and the security industries probably do a lot of—

Mrs. Philippa Lawson: Absolutely, and if businesses do, then there is not going to be any problem. What PIPEDA does is it takes an industry code of practice, developed by industry, and just turns it into legislation so that perhaps the minority of bad actors out there are also caught. The good guys are following their own codes of practice and doing the right thing—common sense, respecting their customers' privacy, not getting into trouble. The legislation is necessary to go after the other guys, the big data brokers who are just ignoring people's privacy. That's more what it's there for.

I can see how it seems really daunting when you don't know the legislation; it's new, and you suddenly feel, oh my God, I have to have a privacy policy, I have to be careful, I have to have all my records in locked cabinets, and that kind of thing. But I think when you go through it, most of it is actually just common sense. In this day and age, when we're suddenly now in an environment where information is so easily available and traded and lost and shared and abused, we just need to, all of us—and this act only applies to commercial activities, but I think there are other activities that we also need to be very careful about—make sure that our computers have passwords, encryption, or whatever, on them to protect the information.

You do need to make sure that if you decide to make secondary use of that information, let's say, in a car dealership.... I know you have my file there, and I know you might contact me in the future about something. I'm your customer, that's fine. But if you then want to sell it to someone else for some other purpose, then I want to have the option of saying no, and I think I should have it.

That's what PIPEDA does; it gives me that option.

The Chair: We'll have Mr. Peterson followed by Mr. Keddy, and that will be the end of round two.

Hon. Jim Peterson: Ms. Lawson, your study of 64 online retailers showed that about half of them actually dispose of personal information to third parties, not necessarily affiliates, and that 78% of those people use opt-out methods for obtaining consent. Would you care to comment further on this?

● (1655)

Mrs. Philippa Lawson: Yes. Opt-out consent is absolutely the standard in the marketing industry. It is allowed under PIPEDA.

Hon. Jim Peterson: Do you think we should allow it?

Mrs. Philippa Lawson: That's a very good question. It was asked earlier, I think, too. I think it's used in situations where it's inappropriate. I think you can do opt-out consent well if you give people proper notice, if you tell them up front, and if you bring it to their attention, effectively—

Hon. Jim Peterson: We're going to sell your personal information to other people unless you tell us not to.

Mrs. Philippa Lawson: I think opt-in is a much better approach, and I think organizations should be using opt-in. I think they're getting away with uninformed consent and consent that's not meaningful consent, because in many cases they're using opt-out and they're not doing it properly.

Hon. Jim Peterson: The Privacy Commissioner says that you don't have to name people, that the threat of naming people gets them to comply. Do you have any comment on that?

Mrs. Philippa Lawson: It doesn't seem to be working. I think the threat of order-making powers might help, but I think organizations are seeing right now a policy of not naming names, so they're feeling quite comfortable that they won't be named.

The Chair: Does anyone else want to answer that? No. Thank you.

Hon. Jim Peterson: Do you think there are fairly widespread breaches of PIPEDA right now?

Mrs. Philippa Lawson: That's what we found in our study, yes.

Hon. Jim Peterson: That's very interesting. We'll want to talk to the Privacy Commissioner about that and what to do about it.

What is the cost of a court case if I feel that I can't get justice from the Privacy Commissioner?

Mr. John Lawford: We have one experience that's fairly detailed, the Englander v. Telus case. In that case, Mr. Englander lost at the trial division of the Federal Court and was ordered to pay, I believe, $15,000 in costs to Telus, and that didn't include his own time. He had to go to the Federal Court of Appeal, and he eventually got his costs back. But I'm assuming that he had more time on top of that. I don't know how many hours he spent on it, but if he was billing himself out at $200 an hour, that would be an awful lot. I know there's another case, which is detailed in our report, of a lady who had to abandon it because the costs were getting too high.

It's like any other court case; it's in the thousands.

Mrs. Philippa Lawson: Tens of thousand.

Mr. John Lawford: Tens of thousands.

Hon. Jim Peterson: If later I complained and disagreed with the Privacy Commissioner's ruling, if she had order-making power, my remedy would be to go to the Federal Court.

Mr. John Lawford: But you'd have the order.

Mrs. Philippa Lawson: Right now the only way to get a binding order is to go to Federal Court.

Hon. Jim Peterson: Thank you.

The Chair: Thank you, sir.

Mr. Keddy.

Mr. Gerald Keddy (South Shore—St. Margaret's, CPC): Thank you, Mr. Chair.

Welcome to our witnesses.

I'm not a usual suspect on this committee, so most of this information is news to me today. I do appreciate the information that you're bringing forth.

I can't quite figure out why we're not acting in a more proactive way to deal with a number of these issues. I suspect there's nobody at the table here who doesn't know someone whose identity has been stolen, and at this time there's no recourse for the individual when this happens.

Certainly the way we do business has changed, the way we store information has changed, and the way we deal with that needs to change to catch up.

I find it a little incredible that when information is compromised, there is no responsibility on behalf of the company, if I understand this correctly, to let the individual know there's a possibility that their personal information could be in the hands of someone who wants to use it for criminal or other purposes. Is that correct? All right.

To fix that single issue is not rocket science. I'm not saying this entire act can be corrected overnight, but hopefully some of these issues can be singled out as being more important and timely than others, and corrected. Have you tried to do that?

● (1700)

Mrs. Philippa Lawson: Absolutely.

Actually PIAC and CIPPIC have been calling for data breach notification for a couple of years now. About two years ago, we put out a news release on this and sent it to all MPs, hoping that some action would be taken.

The Ontario government put a data breach notification requirement into its health privacy law. This is the only one that exists in Canada right now. It's an obvious measure that needs to be in place in the context of identity theft. I absolutely agree with you that it's something that can be done quite easily.

We will be coming out with this working paper. As the honourable member suggested, there are a number of details that you need to work out. What is the threshold, the trigger for the notifications? How should the notifications be made? When? Should the Privacy Commissioner be notified? Should the police force be notified, and so on?

I would recommend having further consultation on this. I think there is pretty widespread recognition that this is needed.

Mr. Gerald Keddy: I always marvel that politicians—certainly the previous government, and hopefully we'll be able to correct that—bring in legislation without sunset clauses, without a three-, four-, or five-year period, when we go back and look at that legislation to see if it's done what we wanted it to do—whether it's been effective and whether it's working or not. But that would go along with it.

The other thing I want some clarification on is personal information transfers when a company is sold. If I own a company and have a fair amount of personal information belonging to an individual—and I'll take the example from Mr. Van Kesteren of selling cars—I would need a certain amount of that personal information about previous customers, because there might be a recall. There may be reasons why I should have that.

However, whether or not one has the ability to sell the customer list should be something that would come back to the customer. I don't know how exactly that's handled under the legislation now.

Mr. David Stark: In the legislation, PIPEDA doesn't really address the issue of business transfers. I believe that by contrast legislation in B.C. and Alberta addresses them, and so there's a gap there. I think we need some clarity around what organizations should or should not be permitted to do.

At our company, we filled the gap by putting an explanation into our privacy policy that, should our company be acquired, this is what we would require of the acquiring company.

Mr. Gerald Keddy: Where I'm trying to head here is, do we need clarification on? I'm not questioning the fact that companies need to transfer information. Most companies work and produce a profit on information. But if that information is going to be used for a different purpose than what the customer already understands that it's being used for, then it should be automatic that the customer or client has to be contacted and told, there could possibly be a difference in how we use your information. I'm shocked that it's not there.

Mr. David Stark: Absolutely.

Mr. Gerald Keddy: I'm shocked it's not there. That would sound....

A witness: It is there.

Mr. John Lawford: It might actually be covered by the provision that says, if you change the purpose, you have to give new notice. But we haven't seen a case yet.

Mr. Gerald Keddy: Do you have specific examples? You mentioned the provincial laws that British Columbia and Alberta brought in after the federal laws were passed, where they were able to look at the federal act and make specific changes to correct deficiencies, if you will, within the federal act. Do you have specific examples of things they've done differently from what the federal act has done?

Mrs. Philippa Lawson: The business transaction is one. We have pointed to their provisions on consent, whereby they have very nicely distinguished among three different kinds of consent: the opt-in, the preferable upfront, positive opt-in consent, which is the standard; then the concept of implied consent, where you can reasonably assume the person has consented, given the facts and the circumstances, and where the person would have consented had you asked them, and that kind of thing; and then the concept of opt-out consent or negative option consent, where you're providing notice to the individual and then assuming their consent unless they opt out, and giving them some method for opting out, and by so doing, they have been able to structure the criteria for each of those kinds of consent. It's much clearer in those acts than it is in PIPEDA, although I think the same thing was intended.

The Chair: Mr. Keddy, you're out of time.

We're into round three. I want to remind colleagues it's 5:05. Your steering committee met yesterday, and there is a report of a work plan they prepared, and it's unanimous. It would be nice if we had enough time after this meeting, before 5:30, to discuss that steering committee report. I bring that to everybody's attention.

Unless the clerk sees someone else, at this point the only person on round three is Mr. Tilson.

Away you go, Mr. Tilson.

● (1705)

Mr. David Tilson: How do you know if there's been a breach?

Mrs. Philippa Lawson: Of the act, or are you talking about—

Mr. David Tilson: A breach of the legislation. We've talked about the requirement that businesses or corporations or individuals have an obligation to report breaches. What if they choose not to? What if they decide not to tell on them?

Mrs. Philippa Lawson: Then you don't know.

Mr. John Lawford: At the moment, the act is set up to wait for people to complain. There have been quite a number of complaints. The Privacy Commissioner probably has figures in the annual report. It's not perfect in the sense that if no one complains you don't find out it's true.

Mr. David Tilson: So it's sort of catch-as-catch-can.

Mr. John Lawford: It is.

Mrs. Philippa Lawson: Sir, I think that is the very reason it's important to allow groups like CIPPIC and PIAC to do the kind of research we do and find important non-compliance and complain about it, because privacy breaches are so hidden by their very nature.

Mr. David Tilson: Yes.

A number of questions have been asked of you with respect to the order-making powers. Are you suggesting the commissioner have the order-making powers or are you suggesting there be a separate tribunal?

Mr. John Lawford: We're suggesting the provincial model in B. C., Alberta, and Quebec be followed, whereby the commissioner himself or herself has that power rather than a separate tribunal, which we think would be awfully cumbersome.

Mr. David Tilson: What would be the additional cost?

Mr. John Lawford: For a tribunal?

Mr. David Tilson: No. For the commissioner to have that power, because she said she doesn't want it.

Mr. John Lawford: And we're not quite sure of the reasons.

Mr. David Tilson: I keep looking at over $16 million. That's what I keep looking at. I'm wondering what the next bill is going to be if you get into an order-making power.

Mr. John Lawford: I don't see the difference between writing a finding and writing an order. It may be a bit longer, it may be slightly more costly, but they were doing the work anyway, so let's make it effective.

Mr. David Tilson: Now, you get into the issue—and it's been mentioned briefly—where you have an individual and there's a hearing, I would assume. I don't know how that would take place. Maybe you have some ideas as to how that would work. There would be an investigation, presumably, and then a hearing. I guess the commissioner would make the investigation and make an order. Is that what you say is order-making? If she found there was a violation, there would obviously have to be a process set up whereby one could defend oneself.

Mr. John Lawford: That would be an improvement on the present situation, whereby the investigation has occasionally been a little bit one-sided for either the complainant or the company. We would welcome a slightly more formalized procedure, and as to whether that would add a lot to the cost or not, I don't think so. I think the B.C. and Alberta models have shown you can give people a chance to do written submissions, at least, and I'm not sure if they do oral as well. We don't want to judicialize it overly, but—

Mr. David Tilson: You get into the issue of one who doesn't like the decision of a commissioner. I'm just following along on your philosophy, because a number of people have come to us and said the ombudsman approach is better than the order approach. It's almost like being a judge and prosecutor at the same time.

Mrs. Philippa Lawson: Can I answer that?

That's absolutely right. There's great merit to the ombudsman approach, and we're not saying to get rid of it. We're saying to continue the ombudsman approach and resolve as many of these disputes as you can through mediation and that sort of thing. But you should also have the order-making power for those kinds of issues for which it is appropriate and for those that need the order-making power.

Mr. David Tilson: If she had that power, it has been mentioned that presumably there would be the capability to appeal that to another place. We've talked about the cost of that—and I think you're actually a little low in your cost, but that's all right.

Have you contemplated whether there should be issues where the commissioner...? I'm thinking, for example, of the court system, of small claims court claims that are non-appealable unless the quantum is over a certain amount. Is it possible to categorize minor types of offences so that decisions on those could not be appealable one way or the other?

● (1710)

Mrs. Philippa Lawson: I haven't thought about that.

Mr. John Lawford: We haven't thought about it in detail, but take, for example, the very garden variety company that didn't respond to my request for what information they held on me or didn't respond within thirty or sixty days or whatever it is under the act. Those are the sorts of things that would be more difficult to appeal, so they might be appropriate. But I would like to look at it more before we make a proper answer.

Mrs. Philippa Lawson: Can I respond to the broader issue? The Alberta and B.C. models make the commissioners' findings final. They're not actually appealable to court.

Mr. David Tilson: Ever?

Mr. John Lawford: Judicial review.

Mrs. Philippa Lawson: There's always the possibility for judicial review. That always exists. It may be that what you're talking about is applications for judicial review. But those are the models that we've been proposing.

We've also proposed a simplified procedure. The Federal Court does have, in its rules, rules for simplified procedures. I haven't studied them to see how effective they are, but absolutely, a lot of these cases are susceptible to written evidence and simplified procedures. We should structure this in a way that is most efficient, with the lowest cost for everyone.

The Chair: Mr. Keddy.

Mr. Gerald Keddy: Thank you, Mr. Chair.

I want to go back to where I left off in the last line of questions, and that was the B.C. and Alberta examples. You've had the two provincial jurisdictions come in after a federal act, with the ability of hindsight to look at and see how the act has been applied. I do have some concerns, as Mr. Tilson has. We don't want to create a bureaucracy that becomes this omnipotent bureaucracy all by itself, that actually over-complicates the act and forces people to the last recourse of litigation for every single issue. That would be something I would fear.

In B.C. and Alberta, because they've had the advantage of hindsight and the ability to look at the act as it was written, has the incidence of litigation gone up, has it gone down, or is it the same? Do we know?

Mr. John Lawford: I don't think we know at the moment.

Mrs. Philippa Lawson: You'd have to ask them. I'm just trying to think of any court cases that I'm aware of in those two provinces. There may be some, but I'm not—

Mr. Gerald Keddy: If you're advocating change at the federal level, that's a piece of information that we really should have to see how it's applied on the ground. That's one of the cases, at least for me, where I'd want to know if it has worked on the ground in B.C. and in Alberta.

Mr. John Lawford: We'd love to know too.

Mrs. Philippa Lawson: Both of those are being reviewed. The Alberta legislation is currently being reviewed, and the B.C. one is about to be reviewed by the legislature.

Mr. Gerald Keddy: There's a prepared question here that deals with the B.C. Information and Privacy Commissioner. He stated that he would not support an explicit notification requirement along the lines of those that have been happening in the United States. He would prefer to wait for evidence that mandatory notification is actually a cost-effective way to reduce risk of, for example, identity theft flowing from a so-called data breach. In the meantime, he's saying it would be better to reconsider the PIPEDA obligation for organizations to take reasonable security measures to protect personal information against unauthorized use and to work with organizations and issue guidance.

Do you have a comment on that? Where does that come from? It just seems to be contrary to what they're doing.

Mr. John Lawford: It seems out of the blue to me, and we think it would be an incentive for people to do better security, because they then have this requirement.

Mr. Gerald Keddy: I'm not in disagreement. I'm wondering where that came from.

Mrs. Philippa Lawson: I think I know where it comes from. The B.C. Information and Privacy Commissioner had an experience with a particular data breach example involving a local mental health organization that had files on the psychiatric conditions of many people. There was some breach. Something happened and they didn't know who got the information, so they felt they needed to notify all these people. In that situation the B.C. Information and Privacy Commissioner was involved, and there were all sorts of difficult questions that needed to be answered. Would the patients themselves be further traumatized by receiving the notification? How would they be notified? The details of going about the whole thing were difficult.

I think it was that particular experience with a mental health organization that led him to question whether we want to jump into this. Of course, I would recommend asking the question directly to him.

● (1715)

Mr. Gerald Keddy: Just for my own personal revelation here—and I apologize for not knowing this file really well—are there different levels of offences, different levels of business? If I'm the Canadian Imperial Bank of Commerce, quite frankly, then I need to have encryption and I need to have a series of protective measures in place to protect your and my personal information. If I'm delivering something from door to door in sales and I have an address and a name or a phone number, I need another level of protection to protect my client's information. Is there a clear differentiation for that under the act?

Mr. John Lawford: It's not that clear, but there is a principle that says you have to take physical, organizational, and technological measures that are appropriate to the sensitivity of the information.

Mr. Gerald Keddy: So if you're keeping information in a scribbler, take care of it and don't lose it.

Mr. John Lawford: Yes. And if you're a large bank, you have to do encryption and have security personnel, and I think the Privacy Commissioner recognizes that.

Mr. Gerald Keddy: She recognizes that there's a difference?

Mr. John Lawford: There's a level.

Mr. Gerald Keddy: I'm sure what all my colleagues would—

The Chair: Mr. Keddy, that's five minutes.

Mr. Van Kesteren.

Mr. Dave Van Kesteren: Thank you, Mr. Chair.

Mr. Keddy has probably gotten some of my questions answered. Again, I just want to pick up where I left off.

I serve on the industry committee as well. One of the foremost concerns of industry today is that they're just laden down with so much bureaucracy. Are we witnessing the birth of a bureaucratic nightmare? That's my biggest concern.

I've heard all the witnesses say, too, that they have this in place and it shouldn't take more than a little bit. But if you've been in government for a while, you know things just don't happen that way. They just have a tendency to grow. I'm wondering if this is all necessary.

I'm just reading some of the other suggestions too, and I don't know if anybody has brought this up yet. The CSA code was suggested. Can you comment on that? Is it something that would make this a whole lot simpler?

Mrs. Philippa Lawson: The CSA code has become PIPEDA. PIPEDA is the CSA code, basically.

Mr. Dave Van Kesteren: So they're using those standards?

Mrs. Philippa Lawson: That's exactly it. PIPEDA is really just legislating good business practice that has been recognized by businesses.

I can certainly say, for myself, that when we were coming up with these recommendations, I was taking the kinds of concerns you're raising now very much into consideration. The last thing we want to do is create more bureaucracy and more expense from it, but what we want to do is make it more effective, in an efficient way. We've tried to design the recommendations here in a way that doesn't require more expense or effort on anyone's part. They will for sure on the part of the Privacy Commissioner, and they will require expense on the part of private businesses that are not currently up to shape in terms of their privacy protection practices, but they should be.

Mr. Dave Van Kesteren: Just to go back to the point that we were discussing the last time I was flooring some questions, isn't public education a solution too? Isn't it just something as simple as telling folks that when they're playing on that computer...? We do that all the time. The government has advertising. Wouldn't a solution like that be just as efficient?

Mr. John Lawford: It's a big part of the solution, but it is only part. We can see, just from the cases we've had in the last three years, that one part of the solution is convincing businesses to change certain business practices that have been found to be privacy-invasive and that they're not changing.

But a big part of it definitely would be getting the consumer up to speed on what the act requires.

Mrs. Philippa Lawson: A lot of what's required here is just pure transparency. It's saying to businesses, tell the consumers what you're doing. Don't do it behind the scenes; tell them if you've had a data breach and that they might be the subject of identity theft.

These are all pretty common-sense kinds of things that I think most businesses who have thought about it are already doing, or would do in those circumstances.

● (1720)

Mr. Dave Van Kesteren: Thank you.

The Chair: Mr. Tilson.

Mr. David Tilson: Getting back to the order-making capabilities, my understanding is that the only major order-making capability the commissioner has now is to identify a company that's breached something, which I think Mr. Lawford said she has done either not at all or once.

What happens if there's been an identity theft because of some action of a corporation or individual, and it's been established that the identity theft was caused by confidential information being released? And when you say order-making power, are there any suggestions on what other penalties there should be?

I'm thinking specifically of a very serious case where someone has stolen someone's identity and the most you can do is say, “Oh, the company breached it,” because that's all there is.

Mrs. Philippa Lawson: We've actually recommended that this be treated as an offence and that there be a penalty for that.

Mr. David Tilson: What would that be?

Mrs. Philippa Lawson: I don't think we've explicitly specified the penalty. It's something that needs to be further discussed, but we've said that should be subject to sanctions.

Our recommendation nine suggests that the offences section be expanded. On data breach notification, our recommendation is that there be tough penalties for that and not simply injunctive relief, which is appropriate for other kinds of problems.

Mr. David Tilson: And you think that would be all right if you didn't have an appeal from those? I gather you're recommending what the other provinces have, no appeal.

Mrs. Philippa Lawson: We have two different things here. We have the commissioner's orders and we have offences. Offences are prosecuted by the attorneys general.

Mr. David Tilson: Oh, I'm sorry, you're going somewhere else here.

Mrs. Philippa Lawson: They would be treated as different categories. Those are not orders that the commissioner makes.

Mr. David Tilson: Okay.

If we decide that we're not going to agree with you and that there shouldn't be order-making powers, and we continue on with the ombudsman model, what, if anything, should one do to improve that?

Mrs. Philippa Lawson: Recommendations three to eleven in our submission are all about that.

Mr. David Tilson: I haven't had a chance to look at those.

Mrs. Philippa Lawson: I can quickly run through them.

Mr. David Tilson: That would be helpful.

Mrs. Philippa Lawson: We're saying that there are lots of things you can do here to improve the situation.

You can make it easier for individuals to take cases to Federal Court, to get binding orders and damages where they have suffered damages. They should be protected from adverse cost awards in Federal Court unless they've behaved irresponsibly. They should be eligible for solicitor-client costs if they win. There should be the possibility for punitive damages, not just compensatory damages, in appropriate cases. Privacy breaches often don't carry much in the way of compensatory damages, and yet we would all agree that there's a behaviour here that should be punished.

We've talked about the publication of names. Permitting class actions is another important one. Right now only individual complainants can take their matters to Federal Court. They have to get a finding from the commissioner, and once they have that they can go to Federal Court. But often what we're talking about are breaches or violations of the act that affect thousands of individuals. The act should allow class actions in those situations. The Federal Court has rules for class actions that can be structured to permit those kinds of proceedings in appropriate cases.

The commissioner is doing a pretty good job of reporting statistics in her annual reports right now, but there's probably room for improvement. That should be mandatory in any case. It shouldn't be a discretionary thing. We need to know, particularly if she doesn't have order-making powers, more facts about what's going on.

We talked about audits, and we talked about expanding the offences section.

All of those things you can do without creating order-making powers.

● (1725)

Mr. David Tilson: Okay, thank you.

The Chair: Thank you, Mr. Tilson.

Mr. Keddy.

Mr. Gerald Keddy: Thank you.

Again, it would seem to me that the request to appear here and to actually have some straightforward, fairly basic changes made to the law that protects consumers would be a responsible task for government to certainly look at and assess. I'm surprised that it hasn't already been done, quite frankly. I realize that maybe the act has only come into play in 2004, but you said it has been here since 2001. I'm just looking at some of the points, and I will repeat them, because I think they deserve to be on the record.

It's actually quite shocking that a large proportion of online retailers, one-half to two-thirds of your sample, share consumer information with other companies for purposes beyond those necessary for the transaction or service in question.

I can't imagine that people aren't absolutely up in arms over that.

Mrs. Philippa Lawson: They don't know.

Mr. John Lawford: There's a little bit of pushiness in principle 4.3.3 of the act that says it has to be for a legitimate and explicitly mentioned purposes, but we think that gives too much wiggle room, and we would prefer to have it amended so that it has to be information only requested for providing that service. That's why we said, here is a technical amendment, but we're shocked as well.

Mr. Gerald Keddy: Surely even if all of us are not up to speed on it, we all understand that we are in the information age, and information has value and you call sell lists. That's a value.

That's a value that's not taxed, in many instances. There's no record of it, but with most of those transactions, there's a whole economy that works around information and delivering information, and even around the protection of information. Obviously, if 78% of retailers rely on opt-out methods to obtain consumer consent to secondary uses or disclosure of their personal information, that's kind of a flagrant misuse of the law, as I understand it.

Mrs. Philippa Lawson: I would say it's fine, it's perfectly legal, and it's okay if—if—they are getting proper consent. There are ways of doing proper opt-out consent, but our study shows they are not.

Mr. Gerald Keddy: That's certainly what's inferred in the statement.

The Chair: Mr. Keddy, it's 5:29. Do you have a short, final question that the witnesses could respond to?

Mr. Gerald Keddy: Yes, I do. I think you guys should have been here a long time ago, and this is something that should have been resolved a long time ago.

I have a good friend who had her identity stolen. She went through hell and high water to get it straightened out, and none of her debt was paid by anyone but her—not by any of the people who broke the law.

Mrs. Philippa Lawson: The law is well behind the industry and the technology in this area, and it needs to catch up.

Mr. Gerald Keddy: It was years getting settled. It was unbelievable.

Anyway, thank you.

The Chair: Thank you very much.

The natives are restless. On behalf of the natives, I want to thank the witnesses, particularly for their specific recommendations. It is always very helpful, and we do appreciate that.

Thank you for your candid remarks and candid answers. We appreciate your coming and we'll do our best to do what we can to make the act better. I'm not sure about order-making powers, but we'll see.

Committee members, we'll be back on Monday. We'll have the Canadian Bar Association, Professor Kerr, and the Information Technology Association of Canada.

I'm sorry, Madame Lavallée, we're out of time.

[*Translation*]

Mrs. Carole Lavallée: I'd just like to have time to—

[*English*]

The Chair: If we'd had time to discuss the steering committee's report, it would have become clearer, but we'll continue to meet until such time as the House adjourns.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca
