House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 018 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Wednesday, November 22, 2006

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Wednesday, November 22, 2006

● (1550)

[*English*]

The Vice-Chair (Mr. David Tilson (Dufferin—Caledon, CPC)): I call to order the Standing Committee on Access to Information, Privacy and Ethics, pursuant to an order of reference of Tuesday, April 25, and section 29 of the Personal Information Protection and Electronics Documents Act, statutory review of the act.

I apologize for our lateness, but there were some things going on in the House.

Today we have as witnesses Richard Rosenberg, the president of the B.C. Freedom of Information and Privacy Association; and Colin J. Bennett, a political science professor from the University of Victoria.

Welcome to Ottawa.

We normally start off with a few introductory comments from the witnesses, and then there are questions from the different caucuses.

You may begin.

Mr. Richard Rosenberg (President, B.C. Freedom of Information and Privacy Association (FIPA)): Thank you for the invitation.

I represent two organizations here, actually, the B.C. Freedom of Information and Privacy Association and the B.C. Civil Liberties Association.

On February 9, 1999, I appeared before the Standing Committee on Industry to present my views on behalf of Electronic Frontier Canada on Bill C-54, PIPEDA.

We supported the bill in principle. Now, on behalf of BC FIPA and BCCLA, I wish to renew our support for privacy protection in Canada by means of PIPEDA. However, there are a number of issues that must be addressed in order to ensure that the privacy of Canadians continues to be protected by this important piece of federal legislation.

In this submission, I will address a number of issues related to both the legislation itself and the operation of the Office of the Privacy Commissioner.

It's important to emphasize that privacy rights are increasingly under attack, and a necessary bulwark in defence of these rights is at the very least adequate legislation supported by a vigorous agency to defend privacy rights and to draw attention to current and anticipated problems.

The most important recommendation I will make in these notes is that the current ombudsman model for conflict regulation employed by the OPC be replaced, providing the minister with order-making powers.

I draw your attention to a story that appeared early in November in the newspapers, in which the British Broadcasting Corporation, the BBC, reported that Richard Thomas, the information commissioner of Britain, had referred to Britain as "waking up to a surveillance society that is all around us".

Some of its characteristics are given as follows: by 2016, shoppers could be scanned as they enter stores; schools could bring in cards allowing parents to monitor what their children eat; and jobs might be refused to applicants who were seen as a health risk.

The report referred to above is a report on the surveillance society, and I take this as a very serious report. Britain, of course, has been described frequently as one of the most surveillant societies in existence.

To set the tone of some of the remarks that follow, let me turn to some comments I made a little more than six years ago, about the time PIPEDA was approved. I gave some examples of privacy invasions. I argued that one of the reasons for having a law in Canada was that it was necessary that both companies and government be responsible in their privacy activities, and that there be a possibility for questioning the privacy activities, and that the legislation could and should provide this.

Let me describe some of the concerns I have, and I think that will be the focus of my remarks. I have nine concerns, the first of which I'm calling publicizing complaints.

For the most part, the Office of the Privacy Commissioner, the OPC, has decided not to reveal the names of complainants, nor the organizations and companies against which complaints have been launched. It appears that under the current regimen there is little cost to companies that do not resolve their privacy issues; not properly implementing a required privacy regimen is just a small cost of doing business. Public attention would be a much more effective means to achieve compliance.

Second, a much more effective education function is required. The OPC could serve a more effective role than it has up to now; namely, to bring the office and its role under PIPEDA to the attention of the Canadian public. In my classes and talks I have rarely found anyone who knows about Canada's privacy law, his or her rights under the law, or the existence of the OPC, the current Privacy Commissioner, or the activities of the office.

A survey commissioned by the Office of the Privacy Commissioner in March of this year showed that something like 8% of Canadians had heard of PIPEDA. Clearly, if you're not aware of laws protecting you, it's going to be hard to take advantage of the protection they provide.

My third concern is the response of companies to breaches of their security. What, if anything, should companies be required to do when their security barriers are breached, with a resulting release of personal information? Such events have become fairly frequent, and most of the attention has been directed towards companies whose primary activity is the collection, compilation, and marketing of personal information.

When PIPEDA came into effect, the term “identity theft” probably was little known. Now ID theft is well known as one of the major crimes associated with Internet technology. In the body of the submission, I include a table showing the numbers of breaches that have occurred in the U.S. in the last couple of years.

The fourth point is on the transborder data flows of personal information of Canadians. The OPC has brought this issue to the attention of the Canadian public, especially with regard to the possible access to the personal information of Canadians held in the U.S. by the FBI under the U.S.A. Patriot Act. In 2004 this issue arose in British Columbia because the government had outsourced medical records to a subsidiary of the Maximus corporation, a U.S. company. It took B.C. Privacy Commissioner David Loukidelis's holding of hearings to find and determine what threats might occur because of this activity. Very briefly stated, the B.C. government introduced and passed legislation in response, which had some of the following requirements: no remote access to data from outside Canada; special restrictions on data access; and requirements for supervision of U.S. employees. I have more listed here. What's important is that the federal government has to deal with these possibilities as well.

Number five, on workplace privacy issues, PIPEDA does not cover information collected by employers about non-federally regulated private sector employees. Workers in three provinces—B.C., Alberta, and Quebec—have protection in the workplace, but basically there is a real lack of it. I should add, for full disclosure, that a researcher and I did a six-month research project for the Office of the Privacy Commissioner on workplace privacy, and we submitted a report to that office expressing our concern about the future of the rights of workers in Canada.

Number six is the development of the electronic medical record, the EMR, and its privacy implications. We recall that when PIPEDA was enacted, the application of the law to the protection of medical records was postponed for one year in order to provide for additional consultation to deal with any special issues associated with such records. I take medical information to be the most sensitive of all personal information and deserving of the highest degree of protection. We're now in the process, across the country, of instituting information systems that will contain, in part, the medical record of every patient who has been involved in the medical system.

Some serious questions arise as to who has access to this medical record and to what degree patients have a chance to say yes or no. One very simplistic model has most of the information about drugs and so on, or about visits, which are not of the most sensitive nature, being available in general without any special permission, but that particular information that's most sensitive might be considered to be in a special lock box, so that only when a patient gives direct permission can that information be released. You ask to whom it would be released. That would be to other doctors, to administrators to make sure that the health process is being conducted efficiently, and to researchers who would like to have access to medical records.

Point seven is on the challenges of emerging privacy-threatening technologies. The law, generally speaking, always seems to be behind new technologies that appear and have good uses, and all of a sudden they start applying to areas that hadn't been thought of. Obviously the law will still apply, but to try to figure out what's going on is the difficulty. I bring your attention to RFID technology, which is being used in U.S. passports. It's part of inventory control, and it also has possibilities for more sinister use. I don't think that's too strong a word.

Let me read you this story, which appeared earlier this year:

> A Cincinnati video surveillance company CityWatcher.com now requires employees to use Verichip human implantable microchips to enter a secure data centre. Until now, the employees entered the data centre with a VeriChip housed in a heart-shaped plastic casing that hangs from their keychain.
>
> The VeriChip is a glass encapsulated RFID tag that is injected into the triceps area of the arm to uniquely identify individuals. The tag can be read by radio waves from a few inches away.

If it had slightly higher power it could be read from several metres away.

How do you feel about this? How should a privacy commissioner act in response to these kinds of activities? There is now talk about medical records going on chips to be implanted. Then you can't forget things, and you'll have this medical record. This is just one of the kinds of technologies to which we're really going to have to pay attention.

● (1555)

My eighth point is on current views of some aspects of consent. This is a very long area of great concern. Of a document released by the Privacy Commissioner to stimulate discussion, half of it had to do with various questions of access. Who has rights? Is there blanket access? In some of this, there was some concern about access now taking place under various acts of Parliament meant to deal with terrorism, and the requirements to gain information about individuals without informing them it's being taken. The general question is, how much information can you take from people without getting their assent or at least informing them you're taking it? I use the general term “access” to cover many of these things, but there isn't time to go into them in detail.

Let me turn very quickly to the last of my comments, which is where I began. The Office of the Privacy Commissioner of Canada is committed to the ombudsman model of mediation. Complaints are heard, meetings are held, and non-binding recommendations are issued, with the names of all parties almost always concealed. If they are dissatisfied, a complainant can bring the case to the Federal Court at his or her own expense.

Has this model been effective? There's some disagreement in public responses to this question. Certainly the OPC seems to be committed to its current mode of operation. It is significant that in the three other provinces in Canada with their own versions of PIPEDA, British Columbia, Alberta, and Quebec—and of course the Quebec model came in several years earlier—the model used involves order-making powers. That is, complaints are heard, decisions with legal force are made public, and parties are named. So the full force of public scrutiny is serving as a constant light shining on the privacy practices of companies and organizations, for whom negative publicity is not in their self-interest. That clearly is the single most important recommendation I'm making in this submission.

Let me thank you for the opportunity to appear before you on this very important matter.

● (1600)

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): Thank you very much.

Before I call on our next witness, please allow me to apologize to both of you for being late.

I thank Mr. Tilson for taking the bull by the horns and getting the meeting started, and I apologize to my colleagues—though our second report has now been filed with the House. So at least we know that.

Mr. Bennett, you're next up. Please begin.

Prof. Colin Bennett (Political Science Professor, University of Victoria, As an Individual): Thank you very much. I'm delighted to be here and to have this opportunity.

My name is Colin Bennett. I am a professor and the chair of the political science department at the University of Victoria. For 20 years I've been writing about this subject in Canada and overseas. I've been looking at the spread of surveillance and the kinds of problems that Professor Rosenberg has talked about. One of the things I saw as my role today was perhaps to give you a broader international and comparative context within which PIPEDA has to operate.

I want to stress four things in my remarks. First of all, I'd like to talk about that international context. It's important for you to understand that this legislation is one of a complete family of statutes that have been passed over 30 years by western countries. Secondly, I want to talk about oversight and enforcement. In this regard, I have been a complainant under PIPEDA, and I want to recount my experience of that to reinforce some of the things Professor Rosenberg has said. Thirdly, I want to talk about the law and the standard. This legislation is based on quite an innovative model of a CSA standard, and I think that is something that needs to be analyzed and understood. Finally, I simply want to ask the question, is PIPEDA working? I think you're going to get testimony on all sides of this question, and I have some views on the subject.

I did write some remarks, but I understand they have not yet been translated, and I would like the opportunity to make some further written recommendations at a later stage in this committee's hearings

The Chair: Professor, you're welcome to do that. You just submit them in the language of your choice, provided it's either English or French, and we'd be happy to distribute them.

Prof. Colin Bennett: Thank you.

To get to the point of this statute, the first point, a very important one, is that it is about giving individuals the right to control the information that relates to them. For 30 to 40 years now we've been hearing about the way personal information is captured by organizations, by technologies, and that process has gone on. It's an incredibly important human right and value, which virtually every advanced industrial society now has enshrined in law. It's a right and a value supported by public opinion. Consistently Canadians have said that they are extremely concerned about the threats to their privacy.

The basic aims, however, of PIPEDA are not substantially different from those found in other western societies. It's based on a set of principles, which are in schedule 1 of the legislation, that you see throughout western Europe in other countries as well. It's very important to recognize that PIPEDA really has to be seen within this larger international context. In fact, international agreements such as those from the OECD, from the Council of Europe, and from the European Union have influenced the way PIPEDA was drafted, and indeed the way it has been implemented.

The forces that brought privacy to the agenda in Canada in the 1970s and 1980s were no different from those elsewhere. But one thing that was somewhat different here is that we were relatively late in legislating a set of safeguards for our private sector. Most other countries were ahead of Canada. That has had some implications, I think. Firstly, it meant that when this law was drafted it had to take into account what was going on elsewhere. There was considerable pressure from the European Union and from other countries as well for Canada to get its act together and to join that family of nations that had privacy protection statutes for their private sector. Although our law has been shaped by some distinctively Canadian concerns and interests, it's important to recognize that inescapable international context.

The second thing that I think is important to understand about PIPEDA is that before the law was promulgated there was a great deal of activity in Canada by its private sector. There were a lot of codes of practice developed, and indeed the standard itself was negotiated through a committee that involved both the private sector and consumer organizations. Therefore, the theory behind this legislation was that it would build upon activity that was already going on in the marketplace. There would be codes of practice, there would be a standard, and then the legislation would come over the top of that. Those are two very distinctive things about the history of this legislation that need to be kept in mind.

On oversight and enforcement, laws differ in the various countries about how you actually enforce these various privacy principles. In Canada we have, at the federal level at any rate, opted for the so-called ombudsman model, and you will be receiving a great deal of advice about whether that ombudsman model actually works. I have some mixed feelings about it. I think you need to look extremely carefully at the prospect of replacing the ombudsman model with an order-making model that is currently in existence in Alberta and B.C.

I have been a complainant under PIPEDA, and I would like to briefly recount that story for you.

Back in November 2001 I received a product survey through the mail that I believed was not in compliance with the legislation. There had been some media stories about this at an earlier point. I objected to three things in this survey. I objected to the fact that it was distributed as a kind of fact-finding survey, with very little indication there would be any direct marketing involved. I was concerned about the position of the opt-out box on the survey. I was also concerned about the fact that there was no way one could complain, no website, and no 1-800 number. There were some quite precise issues of general legal compliance that really had nothing to do with my individual rights. I was not seeking redress here. I was seeking for the company to simply clean up its act and comply with the law.

The Privacy Commissioner agreed with my complaint, agreed that it was a well-founded complaint, and in fact in some respects went even further. But what happened was a long period of negotiation, quite a period of resistance, a lot of to-ing and fro-ing. And the complainant is put in a difficult position in regard to knowing what to do with the information you have, and whether or not to in fact publicize the name of the company concerned. Therefore, they were stalling, and it wasn't until another complaint came in about this company that there was some resolution of the process.

● (1605)

The lesson I draw from this is that the ombudsman model, which is very good at mediating and resolving disputes between individuals and organizations, may not be very good when you're looking at a compliance model or regulatory model like this, where you're simply trying to get the organization concerned to comply with the law. Therefore, I think there's a mismatch between some of the goals of the law and the ombudsman model that is used to enforce it.

Thirdly, I'd like to just say something about the CSA standard. This is a notable innovation. There was an explicit reason why the drafters of PIPEDA decided to legislate by reference to the CSA model code for the protection of personal information. It was believed that if the private sector had already negotiated this standard, the legislation would do nothing more than force companies to live up to their own rules.

Also, I think it's important to note that embodied within this legislation is a method of compliance. There's a standard there. Any organization can take that standard, go out and be registered to that standard, use it as evidence if there's a complaint against them, and use it as evidence that they're pursuing good practices. There are many ways in which that standard can be used more effectively in the implementation of the law. I have a couple more specific recommendations about that, but I see my time is running out.

Is PIPEDA working? You're going to get a lot of advice on both sides of this issue, but businesses in Canada can be divided into three groups.

First of all, there are those large, high-profile companies that have in fact been leaders on this issue. These were the organizations that, early in the process, developed their codes of practice through their trade associations, and that, in the mid-1990s, participated in the development of the Canadian Standards Association's code. My impression is that while these businesses certainly face important challenges and there are clearly privacy issues there, there is a general compliance. They're not necessary compliant because of the law, but because they largely raised their standards before the act was promulgated.

A second category, on the other end of the spectrum, is the free riders, the companies that deliberately attempt to make money out of the processing of personal information without individuals' knowledge and consent. My impression also is that many of these businesses have either been exposed as a result of PIPEDA or have been put out of business.

By far, the largest category of business is in the middle: companies that process the full range of consumer and employee information, but which have never really been concerned about the issue, nor have they been pressed by the media, by their trade associations, by the Privacy Commissioner, or by privacy advocates, to do anything more than the minimum. They may have made an early effort to get a privacy policy and appoint a responsible person, but have had no further exposure to the issue.

There's a good deal of evidence from surveys that most businesses are not generally aware of PIPEDA and are not generally aware of their obligations. My impression is that they're in that large category of organizations that are in the middle of the spectrum, and to which I think the intention of the law needs to be addressed.

The committee will no doubt receive some testimony that PIPEDA is a heavy-handed piece of legislation. I do not think it is. By comparison, it's quite a light form of regulation. If you compare PIPEDA with equivalent statutes in France, Germany, and other European countries, it really is relatively light. But it does depend on the building of compliance from the bottom up. Indeed, the entire regime was founded on the theory that the CSA standard would build upon existing codes of practice and that the legislative framework would build upon the CSA standard.

I've argued before that this kind of approach has a chance of encouraging a more effective system of privacy protection than would the top-down command and sanction model that is enforced through law alone. I'm still of that view, but I also believe the law needs to be reformed. I also think this committee needs to look very seriously at the powers that the Privacy Commissioner has in order to enforce this extremely important piece of legislation.

Thank you very much.

● (1610)

The Chair: Professor, before we get to questions, you said you had two recommendations with respect to the CSA code. Could you state them for us without any argument or rationale, just as they are?

Prof. Colin Bennett: The CSA code is used as a template at the moment, rather than as an enforcement mechanism. One thing that could be done is more explicit recognition, probably in section 24, that the commissioner may require registration to that standard. It might also be more explicitly stated in subsection 18(2), under which the commissioner is empowered to delegate the powers of audit.

The point is that there's a ready-made enforcement mechanism embodied in the legislation, and I think it could have more explicit recognition in those sections.

The Chair: Thank you.

I just wanted that on the record, since your paper isn't before us and just in case members have questions on those aspects.

We'll start with Madam Jennings, for seven minutes.

Hon. Marlene Jennings (Notre-Dame-de-Grâce—Lachine, Lib.): Thank you, Chair.

Thank you very much for your presentations.

I'm really interested in the comments you've made on your participation in the development of PIPEDA, the hearings that were held before the industry committee when the previous government brought it forward, and the experience of the five years and where you see weaknesses.

Mr. Bennett, you talked about the model being quite innovative in the sense that it was built on the basis of the CSA standards and the understanding that the industries would actually conform to it and build from there. Do you think with that model, which you appear to feel was the right way to go, that possibly the weakness of the legislation is precisely on the commissioner's side in the sense that it is in fact an ombudsman model, and you have large numbers of companies that aren't even aware of the legislation? If they're not aware, how can they comply? Also, a large number of Canadians were not aware of the legislation; therefore, how can they ensure as much as they can that their rights are in fact being respected?

If the commissioner had executory powers, the power to issue orders and order compliance, that would then bring a significant amount of publicity, and there would be a certain level of public education on the legislation both within the private sector and amongs Canadians—what it's about, what their rights are, what their duties are, etc. Do you think that's a missing piece in the legislation?

● (1615)

Prof. Colin Bennett: The commissioner has the power already to educate and to publicize.

There are a number of issues inherent in your question, if I could break them out a little bit. The first has to do with public education. The commissioner can do that right now, and obviously that is constrained by certain resources. Then there's the second question, about the naming of names, the naming of companies that are subject to complaints. That's a tricky one under an ombudsman's model, which is premised on the assumption that there will be mediation and all possible effort will be made to work things out in private.

On the separate issue, however, about order-making power, I think the argument is that if you gave the commissioner powers to make orders, it would undoubtedly change the culture of the office. It would undoubtedly create some tensions between the current Privacy Commissioner's office and the Information Commissioner's office, but it would bring the federal Privacy Commissioner's powers more consistently into those of the provinces. It would, I think, give the commissioner some teeth and facilitate mediation, and hopefully—although I think this needs further study—it would speed up the mediation process. It could cut into costs and delays, and I think it would foster a proper jurisprudence.

That, I think, is the most important problem here, that you can look at the findings.... And I do not wish to appear in any way critical of the Office of the Privacy Commissioner; I have enormous respect for what they're doing. But the current model does not foster a proper jurisprudence—for individuals or for organizations. And that's what you get when you have the more, admittedly legalistic, order-making model.

Hon. Marlene Jennings: It is more legalistic. However, we do have experience in other domains of a situation where you have conciliatory powers and investigatory powers and order-making powers. In fact, I had some experience in that before coming into politics in civilian oversight of law enforcement. The key factor was that before it gets to the tribunal—the quasi-judicial part of it, which is the order-making—the information is completely confidential. At the level of conciliation or mediation, the parties have complete confidence that it will remain confidential if there is an agreement. If, on the other hand, there is not an agreement and the commissioner has to go to order-making powers, then it becomes a public process.

Prof. Colin Bennett: That's correct.

Hon. Marlene Jennings: Then if this committee and the government, whether it's the members of the committee or the government or both, bring forth amendments, there would have to be clauses that would ensure, when it's at the mediation stage, that it is in fact not a public process, that it is confidential, and so on.

Prof. Colin Bennett: Yes.

Hon. Marlene Jennings: My other question is to both of you.

When I sat on the industry committee, we had a major concern about the definitions of “personal information” and “work product information”. We were assured at the time that we didn't have to worry about it, that it's covered under personal information and therefore will not imperil, in the health sector, for instance, companies that actually obtain health intelligence from doctors, pharmacists, etc. And then governments actually use it to develop strategy and so on.

Since then, that definition has been challenged. Luckily, the Federal Court has found that “work product” does not come under privacy and personal information. However, there is a demand now that there should be a clear distinction made in the legislation.

Would both of you, Mr. Rosenberg and Mr. Bennett, be in favour of making that distinction so that it's perfectly clear and so people aren't wasting their money having to make challenges before the courts?

● (1620)

Prof. Colin Bennett: Well, you're right that it's not clear at the moment. It's not clear because there is that exemption in the B.C. legislation.

The definition of “work product”.... I'm very familiar with the case you're talking about, because I have to declare that I did do some work for the company that was involved in this issue several years ago, so I have an understanding of the issue that's beyond my understanding as an academic.

If you take the issue of doctor information versus patient information, there's a clear qualitative distinction between the information that is produced as a result of one's professional conduct and the information that one may have as a patient. It's a tricky issue, and this committee clearly has to deal with it and ensure that there is some consistency.

The worry I have, however, with a broad, unlimited definition of “work product” is that it can have unintended consequences for the privacy rights of employees, because there are work product issues having to do with, say, the keystroke monitoring of employees in offices, or that may have to do with video surveillance. So there has to be some very careful drafting.

I'm familiar with what the Privacy Commissioner of Canada has said and with the various alternatives there. There has to be some very careful drafting to ensure that the legislation does, in fact, specify exactly what “work product” means and no more.

Hon. Marlene Jennings: If the definition—

The Chair: Ms. Jennings, I'm sorry, I can't let you go on. Thank you. That can go on your second round, perhaps.

Hon. Marlene Jennings: Thank you.

The Chair: Monsieur Laforest.

[*Translation*]

Mr. Jean-Yves Laforest (Saint-Maurice—Champlain, BQ): Good day. I am pleased to have you here.

The Chair: One moment, Mr. Laforest.

[*English*]

Are you guys ready for the translation?

[*Translation*]

Mr. Jean-Yves Laforest: We are not all entitled to the same attention.

[*English*]

Prof. Colin Bennett: Excuse me, I'm from British Columbia.

[*Translation*]

Mr. Jean-Yves Laforest: Exactly, since you are from British Columbia, you must be better informed about the Privacy Act of that province.

[*English*]

Prof. Colin Bennett: I'm not getting translation at the moment.

The Chair: You should be on channel 2, I think. Do you have it now? Okay.

[*Translation*]

Mr. Jean-Yves Laforest: You are analysts and managers of the Personal Information Protection and Electronic Documents Act in British Columbia. I would like to ask a few questions of a practical nature. We hear a great deal of talk about laws, regulations and monitoring with a view to determining how the federal act can be improved upon.

First of all, with regard to the protection of privacy, electronic documents or the use of various electronic media, do you get the impression that the general public is sufficiently well informed to understand the different issues and the risks of the various modes of communication?

For example, when citizens use a credit card, a cell phone, the Internet, shop via the Internet, satellite transmissions, etc., do you believe that they are really aware of the risks? Tell me about your experience in British Columbia.

[*English*]

The Chair: We'll let Mr. Rosenberg speak first, since you've been going for a while, Mr. Bennett.

Mr. Richard Rosenberg: Probably not, in general. The Internet itself presents a mystery for most people if they arrive to it without understanding how it operates. For example, a few years ago no one I talked to knew what “cookies” were. They thought it was the usual thing. That's because when we buy a computer, cookies are automatically set as default. You never see the word “cookies”. It's not there. Information is being gathered to every website you visit, and that's not known. Then, of course, you start receiving information. “Spam” has become a common term now for the vast amounts of information sent to people, because information is being gathered from their activities and is unknown to them.

Everywhere you go.... The most common search engines gather information about your searching behaviour. Google has enormous amounts of information about all of us, about how we search, the things we're looking for. The argument, of course, is that they want to improve their methods, they want to be more responsive. That's always the argument for gathering information: it's for your benefit, because you need better access, better quality of information and so on.

The question here is, how do people become informed about all this? Who's going to tell them? Well, you might think you could go to a website and look up the privacy policy of the people who are running the website. They vary from being totally incomprehensible to saying nothing. Mostly that's the case, because most Canadians go to U.S. websites and there are no privacy regulations in the U.S. You depend on the private sector to perform admirably because they don't want a black eye from being accused of something.

● (1625)

[*Translation*]

Mr. Jean-Yves Laforest: Does it not become the role of the government to better inform people, since, as you say, the public is basically poorly informed? Doesn't the government have the important role of advising the public of the risks associated with the use of these various electronic tools? It seems to me that that should be its role, since in the law, we want to monitor e-commerce and the different transmissions.

Wasn't there an oversight in terms of informing the public? Shouldn't the provinces and the federal government, which wants to improve its legislation, examine this major oversight?

[*English*]

Mr. Richard Rosenberg: I think it's not solely legislation. I think what's important—and I think I addressed it very briefly in one of the recommendations I made—is that the offices of the privacy commissioners, both federally and provincially, should have, as part of their responsibility, education of the public about where there are threats to privacy. I think that would probably require more money going into hiring more people to go out and spread the word by a variety of means.

Of course, this ties into other issues about making public the fact that when there are privacy violations, people should hear about them. They shouldn't be behind the scenes and then some newspaper reporter discovers it and tells you about it. This is an ongoing education process. The Internet is a technology, I think, that appeared with such rapidity that there was hardly any time to adapt to it and discover some of the issues related to it.

Prof. Colin Bennett: Maybe I could say something from some of the survey evidence that we have in Canada about what individuals think about privacy.

It is true that the vast majority of Canadians do not know about the legislative protections and do not know about the recourses that are available to them. On the other hand, it is also true that the vast majority of Canadians are extremely concerned about this issue. Vast majorities have experienced serious privacy invasions and a good number understand the issue instinctively. They know that when an organization is capturing information about them that they regard as illegitimate, they have a very instinctive attitude that it's none of your business.

Now, those attitudes will vary by gender, by generation, and to some extent by province, but I think the education is part of a larger set of tools that is needed in order to implement privacy in Canada. This is one of my larger points. The law is only one of many instruments that need to be used these days in order to give individuals greater control over the personal information that circulates about them. One is obviously information and education; another one is a lot of self-regulation that businesses can do on their websites and so on. There are also privacy-enhancing technologies, such as encryption tools, that can be used. The law is simply one part of that set of instruments.

● (1630)

The Chair: Thank you.

Mr. Tilson.

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

It's interesting talking about all this business, because on the one hand these are very Orwellian thoughts.

My friend here is using a BlackBerry, and I understand that if you're in a private meeting you'd better leave your BlackBerry outside the room, because someone can use it as a transmitter. If you have some confidential information, and you're on your cellphone in the Centre Block, you'd better be careful you're not blabbing too much, because someone can pick it up. It's rather frightening. On the other hand, people don't seem too concerned about security at airports, having cameras in convenience stores, banks, airports, because they're worried about their personal safety.

When you're talking about all these things, we say we have to protect our privacy, but on the other hand—and you say the public is concerned about that—the same public is also interested in protecting personal safety and has absolutely no problem being searched at the airport and practically strip-searched at the airport. They are terrified something's going to happen on a plane or other places. They are concerned about going into a convenience store and some strange thing happening there, so they don't mind the cameras being there. Can you go too far either way?

Prof. Colin Bennett: Yes.

With respect, there's a good deal of survey evidence that suggests individuals are concerned about new technologies and their use for surveillance purposes when they do not see a legitimate public purpose. When I talk to audiences, including my students, and I begin to ask them questions about the capture of this personal information, the concerns increase the more they know about the way the technology might be used.

For example, you gave the instance of a video surveillance camera in a corner store. Okay. The general public sees that as a camera. I see it as a mechanism by which personal information is captured, which raises a whole bunch of other questions. How long is that information collected? Who might have access to that information? To whom might it be disclosed? What kind of technology is being used? Is it associated with facial recognition software and so on and so forth?

You have to drill down beneath the basic question about whether the surveillance is happening to find a whole range of very interesting and serious questions that any organization has to address, if it wants to capture personal information in that way. That, of course, is what the privacy legislation tries to get at. It does not say no, thou shalt not collect personal information. It says if you are going to collect personal information, you should be collecting it in a certain way to make sure there's a legitimate purpose and that the individuals about whom that information is collected have some rights associated with it.

Mr. David Tilson: We're talking about the Personal Information Protection and Electronic Documents Act?

Prof. Colin Bennett: Yes.

Mr. David Tilson: In other words, regulating the private sector. To do that, I expect there are going to be groups that come and say to the private sector, you must do this, this, this, and this.

Have either of you philosophized on the concept of what that's going to cost business, either economically or in time? Should we care about that?

The Chair: Let's get Mr. Rosenberg on the record on that.

Mr. Richard Rosenberg: I'm still thinking about your previous question. I want to distinguish between two kinds of surveillance, private and public surveillance.

When I go into a bank and it has cameras, I'm on its property, and it, in using those cameras, has legitimate use and would have to specify, of course, some of the questions Professor Bennett was concerned about: who gets to see it and how long it stays.

The public area concerns me a great deal, because there is endless talk about putting more video cameras in downtown areas of cities. Vancouver is talking about this endlessly. Leading up to the Olympics, we're going to have security issues. They're talking about putting them on Granville Street, the major north-south street in the city. The question here is, has this been sufficiently understood? Is there a cost-benefit analysis? Of course they have to prepare a cost-benefit analysis for the privacy commissioner of the province.

● (1635)

Mr. David Tilson: Sir, if I could interrupt, I understand we're taking about.... I mean, photo radar is popping up again, in Ontario at least, which may or may not be a good thing, but that's for someone else to debate.

My question is, are the regulations that we'd be suggesting to be put on private industry...? And you're right, I did confuse my examples, but let's zero in on the bank or the corner convenience store. They're the only ones I can think of; I'm sure you could think of dozens more.

I guess the cost to those particular businesses, not only economically in time, with respect to what they're going to be required to do.... Because the cost of business is one thing; protection of people's privacy is another thing. Surely you have to consider the cost to those businesses of demanding that they do certain things.

Have you put your thoughts to that, either of you?

Prof. Colin Bennett: Yes. There is a good deal of analysis about the extent to which PIPEDA is costly in monetary and resource terms, etc.

My own view is that the costs of being privacy unfriendly far outweigh those. The costs of having a bad reputation in the marketplace, of being seen as unfriendly to privacy, far outweigh whatever compliance costs there would be in implementing proper security measures, or putting an opt-out box on a marketing form, or so on.

There are exceptions. There have been some companies that have had to invest a great deal into this. But by and large, most companies recognize the value of privacy.

Mr. David Tilson: What do you base this on? Where did you get that?

Prof. Colin Bennett: There are plenty of examples, particularly with identity theft issues, where the stock of a particular company has plummetted as a result of bad publicity. It's difficult to quantify, and I don't have the information in front of me at the moment. I could certainly submit it to you. But businesses want to maintain good reputations, and privacy is a way for them to gain and maintain the trust of their customers.

The Chair: Thank you, Mr. Tilson.

If you have empirical evidence for your comments, we'd be very pleased to receive it, if you wouldn't mind.

Okay, we'll go to Madam Jennings, and then we have Mr. Stanton. If any other members want to ask questions, could you please raise your hands and catch the eye of the clerk, so he can write the names down?

Madam Jennings.

Hon. Marlene Jennings: Thank you, Chair.

I'd like to come back to the issue of a distinction between the protection of personal information and the exemption of same when it comes to work product or professional information.

Mr. Bennett, you said that it would have to be very carefully crafted, in order to ensure that it doesn't become wide-ended. If you put your mind to it, would you be in a position to perhaps—maybe not today—suggest an actual definition that would allow for that distinction to be made, that exemption to be made, and at the same time ensure that it's not overly broad?

Mr. Rosenberg, in your brief you end with a number of recommendations. One of them is that the Privacy Commissioner should have the power to make orders. The British Columbia Civil Liberties Association recommended the power to render orders that could be tabled before the Federal Court and rendered immediately executory. I'm assuming that you're in agreement with that.

The other thing you raise in your brief is the issue of the lack of protection in the workplace for the personal information of employees, for whom that regulation or protection comes under federal jurisdiction. So in that case we're actually talking about in all the provinces and territories that have not brought in their own protection of personal information legislation, and that has been found to be similar to that of the federal and therefore we vacate that jurisdiction.

Do you have a preference...? You know the legislation better than I do the protections that already exist in B.C., Quebec, and Alberta. Do you think that one of those three models is better than the others, or are they pretty much similar in that protection? Because if this committee is going to look at the possibility of strengthening PIPEDA, in order to provide those clear protections, which do not exist, we would need some guidance on what models actually exist that in your view are good models to follow.

Following that, Mr. Bennett, would you like to add to this issue?

● (1640)

Mr. Richard Rosenberg: I think the Alberta and B.C. are fairly—

The Chair: Excuse me, there is one question for Professor Bennett about a specific amendment, two questions for Mr. Rosenberg, and then a comment by Professor Bennett after Mr. Rosenberg.

Professor Bennett, could you address the first question?

Prof. Colin Bennett: Yes.

On the issue of the work product thing, I'm not sure what I would have to add beyond what's in the Privacy Commissioner's paper on that. I'd have to go back to it. I can't quite remember. I think there were three or four different options that were included there, one of which was the way the issue has been handled in Quebec. I'm not quite sure what I could add to that.

Hon. Marlene Jennings: Okay, thank you.

The Chair: Mr. Rosenberg.

Mr. Richard Rosenberg: I think the Alberta and B.C. legislation are fairly similar and the Quebec is different, but I have to admit that I'm not as familiar with the Quebec legislation as I should be.

What I've been concerned with in my research is gathering the variety of ways in which the privacy of workers is threatened. It's not just keystroke monitoring and Internet activity and television or video cameras in the workplace. It's also endless tests that are required of people now for various occupations—drug tests, genetic tests, psychological tests—and these can go on both in the hiring processes and in the ongoing work process. These bring a lot of issues. It will be very difficult to try to figure out how to regulate these in appropriate ways to allow the worker some sense of humanity, without there being this constant threat.

I think a lot of it results from the fact that there is very much a general rubric about technology—if you can do it, why not do it? If it's possible to have a technology that gives you this and this seems to be useful, then do it, and that seems to be what's going on.

I have to say, also, that things are terrible in the States, where there is no privacy protection. Employers basically have complete rights to do whatever they want.

One of the at least temporary measures has been to try to work out a common agreement between management and workers about general rules on how the technology will operate. Are they going to watch everything you do? When you're on your lunch break, can you use the computer in the company without it being monitored? We know that the telephone brought these issues. Is it okay for a worker to call home to see how her sick child is doing? No management would say no, you can't call home. Is it okay to sit at your computer during lunch break and plan your vacation for next year? Well, you're not actually working, then, but it's not your machine, not your software, not your anything. Are you okay with doing that?

There's an endless number of these kinds of issues about which you would think people could come to a common agreement without the law intruding, but it's not the case.

The Chair: Thank you.

We have Mr. Stanton, followed by Madame Lavallée and Mr. Wallace.

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

Thank you to our witnesses today.

To Mr. Rosenberg, the first item that you raise in your list of nine concerns was with respect to the publicizing of complainants. In particular, you said that the public attention on these issues would be, I think, in your words—and I'm paraphrasing here probably—a much more effective means of compliance. Could you expand on that a little bit and perhaps add in there in comparison to what's happening now with respect to these compliance issues? Help me understand better what you mean by that, and bringing that out in the open.

● (1645)

Mr. Richard Rosenberg: I think, by and large, the process in the Office of the Privacy Commissioner is a process about which only the person making the complaint and the organization or company against which the complaint is made really know what's going on. They're the ones who heard the judgment. The Privacy Commissioner will then make a recommendation that can be followed or not followed, because it has no legal force.

There is an option for the complainant to go to the Federal Court and pursue it, which would presumably cost—

Mr. Bruce Stanton: That puts it into a public forum at that point.

Mr. Richard Rosenberg: Yes.

The question is, is this the better way to go and complain? I think Professor Bennett talked at length about this, and there is some debate about what's the best way to go. There's a best way for the complainant and a best way for privacy protection in general.

If you make a complaint now and you are told that the Privacy Commissioner's office upholds your complaint, then what? What should you do? You could hope that the company would take that as a message and clean up its act or do something, but there's no requirement that they do it. So what have you gained by that?

Mr. Bruce Stanton: Do you have any understanding as to why the Privacy Commissioner has opted for the approach that's currently there respecting—

Mr. Richard Rosenberg: It's been operating that way since the beginning. I think it's one of these things where they can make it public if there's a strong public interest; otherwise, it's not. I imagine that not every case would be seen as having strong public interest. It would be very constrained and a very individual kind of process.

I think the basic notion is to do it somehow by persuasion. Basically, if you can persuade companies to improve their operation, without going public, that could be a less tortuous way. I'm not sure. But I think the possibility of improving things is not being pursued as it could be by going public.

Mr. Bruce Stanton: Professor Bennett, did you have anything to add on that topic?

Prof. Colin Bennett: Yes, I have one or two brief things.

The problem occurs in section 20 of PIPEDA. Subsection 20(1) obliges confidentiality in the proceedings. Subsection 20(2) allows the commissioner to "make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so". The commission has interpreted subsection 20(1) as overriding subsection 20(2), under most circumstances. I certainly understand the sensibilities there.

I have a couple of additional points to what Professor Rosenberg said. It does put an extraordinary burden on the complainant. When you receive a finding, and you know the name, and so on.... I recounted my story. I'm in a different position from most people, because I have a certain profile in this community. I have the opportunity to make things public, but most people don't. I don't think it should be up to the complainant to make a decision about whether to publicize the name of that company. There are some complainants, CIPPIC, for example—whenever they make a complaint, they simply put it on their website. That's an approach. Therefore, it's public anyway. You have this bizarre situation where everybody knows who we're talking about, except it's not actually publicized on the Privacy Commissioner's website.

The second thing about the naming of names is this. Often you don't understand the full context of the dispute unless you know what company we're talking about. If you anonymize the name of the organization, it's often difficult to understand exactly what the business practices are. Therefore, as I said earlier, it's difficult to really get some clear jurisprudence about what the law is and whether that would be a precedent for another case that might come along.

Those are the issues. I really do sympathize. They're difficult. It's not easy to simply name names as a matter of course. But so far, I don't think the balance has been struck correctly.

Mr. Bruce Stanton: Thank you.

The Chair: Thank you, Mr. Stanton.

Madame Lavallée, please.

[*Translation*]

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

Good day and welcome everyone.

I am very pleased to meet you, as I have many questions and I am hoping that you can clarify some things for me. I am new to the committee and I also know very little about the Privacy Act.

First of all, one of my concerns is about workers. You spoke a lot about the surveillance of employees while on the job, under the pretext of security. I would like you to tell me if the law prohibits an employer who has installed video cameras to ensure workplace security - I'm thinking of a port, an airport or a convenience store - from using these devices to monitor the work of employees, and then subsequently admonishing them if ever they slack off, for example.

I have a few questions to ask, but I will start with that one.

● (1650)

[*English*]

Prof. Colin Bennett: Thank you for the question.

The legislation doesn't make any distinction between consumers and employees; the information is collected on individuals. It makes distinctions in terms of employment, and the categories of information that are protected at the provincial and the federal level. And there are still some gaps in Canada, I have to say. There are many businesses in Canada where the employee information is not protected by private sector legislation.

Essentially, the test in section 7 of the legislation is whether there is a reasonable purpose for the installation of, in this case, video surveillance; and those purposes have to be explained at the time of collection. The employer-employee relationship is a very different one from the business-consumer relationship. And you'll be receiving quite a bit of advice, I think, about whether or not there should be some special provisions made for employee information.

But to answer your question directly, it is considered a capture of personal information, and it has to happen with the knowledge and consent of the individual, unless it falls under one of the exemptions —that is, if we're talking about a federally regulated institution, such as a bank or another federally regulated undertaking.

[*Translation*]

Mrs. Carole Lavallée: I will give you an example, since I'm not sure that I fully understood.

In a port, for example, where there are video cameras for security, does the employer have the right to use the recorded images to admonish employees who, for example, take longer than necessary to do a job?

[*English*]

Mr. Richard Rosenberg: Usually, yes.

You raised some examples, and there are many, many examples of the kinds of monitoring that can go on, some of which is related to the work process in which employees have rights. I'm not sure this exactly answers your question, but one of the arguments for employers to monitor is that they're responsible for the work of their employees. If I sit at my computer and send out a message harassing some individual, my employer is responsible, because I'm using my employer's equipment on my employer's time. The employer could legitimately say they have a perfect right to monitor, because if they're going to have legal responsibility, they have to show they took steps to be in charge, if you like, and to be aware. And this covers a whole bunch of activities, not just harassment: it could be trade secrets; it could be going to sexually explicit websites and creating problems in the workplace, and lots of things. So those are part of the work process. Clearly the employer has a right to monitor.

The questions that arise are what about how fast the employer is entering data into the computer; what about how long the employee is spending away from the desk, away from the computer; or what about monitoring in rest rooms? Recall the infamous case of Canada Post, which had video cameras installed in the men's and women's bathrooms because of concern about drug usage while people went to the bathroom. There are devices installed to make sure that restaurant workers are washing their hands before they leave. We all say, oh great, we hope they wash their hands, otherwise, who knows?

So there's a whole range of these things, and many have quite legitimate purposes. It would be hard to argue it is an intrusion on the work process.

● (1655)

[*Translation*]

Mrs. Carole Lavallée: Do I still have some time?

[*English*]

The Chair: No.

Mr. Wallace.

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

I'm sorry I missed a chunk of your thing, but the timing has been all fouled up today with some speeches.

I'm new, as is Madame Lavallée, and the only experience I have with privacy at this point has been do we send them a Christmas card or not, and how did we get their name, and all of those kinds of things. And I'm not going there.

The question I have for you, to begin with, is that legislation has only been in place for about five years, to my understanding, because we're coming up to the review. The health part, which can be relatively controversial, and which may be the most important part, as has been mentioned, has only been around for about a year and a half. Are we premature in even reviewing it without having a good sense of whether or not the thing is working for us and where recommendations and changes might be needed? Should we be saying here's some information that we've had from witnesses such as you, but we really need two or three more years of education on the piece on how it's actually working before we can make any real solid decisions?

If you wouldn't mind answering that, I'd appreciate it.

Prof. Colin Bennett: I don't think it's premature. I think the five-year statutory review is a good thing. However—and I'm not sure this is going to answer your question—I think it is going to be difficult to separate out, when you see problems with the legislation or the implementation of privacy policy, whether it has to do with the statute or whether it has to do with the way the statute has been interpreted by the Privacy Commissioner or overseen by the Privacy Commissioner, or whether it has to do with the larger context since September 11, 2001, and the extraordinary pressures as a result of that to capture personal information. We'll help you try to sort through those issues as best we can, but we can't let this hearing go by without mentioning 9/11 and the fact that the world for privacy changed at that point.

Nevertheless, I do think you will hear some very practical recommendations about how you can tinker with the legislation to make it more effective, to clarify certain provisions and to help not only individuals to understand their privacy rights, but also businesses to know what they have to do. My perception is that the vast majority of businesses in this country understand the issue, get it, and just want some clear advice on how to comply, and there are ways the legislation can be amended in order to effect that.

Mr. Richard Rosenberg: I don't think it's too soon either, although I do agree, in part, with respect to health information, we're just in the working stage of building these large systems. An enormous amount of money is going into them. Requirements are being put on physicians' offices. There are still a lot of doctors who have paper files, and that's not going to work in this age. They have to go electronic, which means they have to transfer all that paper into computer files. Then there are a lot of questions associated with that kind of information about access.

I've been attending meetings of the Department of Health in B.C. and that group that's doing a lot of this work on the electronic medical record, and there are a lot of questions now. They're guided, of course, in B.C., by B.C. law, and so far it looks like it will be okay from a privacy point of view, except that there are just a lot of questions about access that are not well worked out yet, about routine access and special access.

As I mentioned previously, medical researchers believe it's their right to get access to whatever they want, as long as you strip off identifying information. A lot of medical research goes to looking at medical records and seeing people under treatment A, compared with people under treatment B, over long periods of time. The question is, if you strip off identifying information, there should be no privacy issue, because you can't identify the individuals, except that this is another technology appearing where work and statistics show it's possible for certain sizes of groups to recover information. You can do it, in part, if you know where people live and they have a certain disease, because there are only a few people who can satisfy those criteria; and even if you strip off the names in advance, it's possible to recover information about them. So we're forced to think more carefully about that, about the conditions under which the information is available.

● (1700)

Mr. Mike Wallace: Based on this review that we're undertaking, and certainly learning, your expectation, then, based on those answers, is that it's more of a tweaking or what the department might call some minor changes, rather than a major overhaul of what we've done over the last five years. Is that accurate?

Mr. Richard Rosenberg: If they move to order-making power, that would be a significant and major change.

Mr. Mike Wallace: I want to ask you about order-making power.

The Chair: You'll have to do that in the next round, Mr. Wallace.

Mr. Mike Wallace: Thank you very much. Maybe the next time you come here—

The Chair: Ms. Jennings.

Hon. Marlene Jennings: Should I be kind to Mr. Wallace? I'll give you a minute to answer Mr. Wallace's question.

Mr. Mike Wallace: No, we're here until 5:30. Don't worry.

Hon. Marlene Jennings: How much time do I have?

The Chair: Five minutes, including the answers.

Hon. Marlene Jennings: Thank you, Chair.

The question of the new move to electronic medical documents raises a lot of questions. You mentioned that B.C.'s model deals with it but that there are still a number of questions that have not been answered. You talked about medical researchers, for instance.

I'd like you to expand a little more on this issue, because I believe that PIPEDA will have to be strengthened in that particular area, and why not benefit from legislative experiences that already exist to perhaps try to answer some questions that the existing legislation doesn't answer in other jurisdictions?

Mr. Richard Rosenberg: Of course, there's a federal institution, which I think is the Canada Health Infoway, which has been providing money and advice, and they've taken the benefits of work in different parts of the country.

It's clearly an area that should have a uniform system so they can talk to each other. Obviously, one of the benefits of an electronic health record is that it could be accessible anywhere. If your record is sitting in B.C., but you're injured in Ontario or something happens and you need the record, it's really important that it's accessible. That would be one of the major benefits.

If you're trying to understand how well certain kinds of medications are working, what the costs really are, and where there are areas of higher cost, there are an enormous number of questions you can answer with an electronic medical record.

The questions that are still of concern have to do with rules of access. In a lot of cases, the simple rules of access will be straightforward. If you're a doctor and you are of a certain category, you can access things at a certain level.

It means information will have to be structured in terms of different levels of sensitivity. It will therefore require different levels of access by physicians, government bureaucrats, ministers, associate ministers, and deputy ministers of health on the kind of information they can get and the permission level they will be at.

As I said, these things are currently being discussed.

I think this is really important. It will obviously affect PIPEDA, because it will regulate these things for the provinces without any other privacy legislation.

I think it goes back to the question on whether we should wait. I don't think we're going to wait. There is such urgency with medical records that we're not going to wait.

For whatever measures are taken in the provinces, I assume provinces that don't have their own legislation will look very carefully at what's going on elsewhere in Canada as they formulate policies of use.

Hon. Marlene Jennings: Do you have anything to add on this?

Prof. Colin Bennett: Very briefly, I come back to the very first point I made, which is that it's obvious the rules need to be harmonized in this area and in other areas. The way our laws have been developed has been to a large extent with a view to harmonization and understanding the principles.

I've demonstrated it in my writing and I can certainly give further evidence to this committee that those principles are in fact extremely uniform. Therefore, what looks like an enormous practical problem of implementation is sometimes less difficult when you actually work through it.

Hon. Marlene Jennings: I have another question on the whole issue of consent.

I'm aware of a study that was done at an institute. I forget the full name of the institute, but the University of Ottawa looked at a certain number of company practices on the issue of consent, implied consent, express consent, and the kind of privacy protection for personal information and policies that these companies have in place.

I was appalled at the results, in part because there was a debate at the industry committee when the legislation was first brought to us at second reading. I think it needs to be strengthened, and I think it needs to be clarified.

The whole issue of giving consent, even when it's express consent to a company to be able to use personal information in a very clearly defined way, involves the whole issue of a company with its affiliates, for instance, that may not be working in the same domain, offering the same service or product and the sharing of that information. It then goes completely beyond that to third parties that are not part of the company “family”.

I had a personal experience with a credit card company, which I did to see what would happen. You get them in the mail, and I filled one out. When it came to the section for consent, I crossed everything out and wrote that they could only use my personal information within their company. They could not share it with any affiliates that had no direct relationship to the issue of my credit and credit rating. The company literally sent the same form back three times, saying they had a problem and needed me to fill it out again.

For me, it was clear that if I filled it out, my personal information, my shopping habits, and my leisure habits would be stripped out. Maybe my name wouldn't be given, but it would be stripped out and sold to third parties for advertising or whatever. I don't think most people realize that.

I'd like to hear whatever suggestions you have, either today or, if you need further reflection, in the future, in writing to the committee through the chair, on how the definition of consent and its different forms can be tightened up to ensure that when people give consent, it's actual consent.

In my view, there should be virtually no implied consent. It should be express consent.

● (1705)

The Chair: Thank you, Ms. Jennings.

Do you gentlemen have any comments on the issue of consent?

Go ahead, Mr. Rosenberg.

Mr. Richard Rosenberg: The parallel of that is the opt-in or opt-out boxes. When you sign on to something, and you don't look carefully, they have already filled in what they would like you to agree to. There are *x*'s appearing in boxes, and I've always objected. This is really something that does require a lot of energy to change. It's clearly an advantage to companies that people don't know this, that they're giving implied consent to various things because the option that the company wants you to choose is filled out already. And I think it has to be mandatory that if they want to use information, you have to give consent explicitly; it's not implicit, for their point of view, that they get it.

Prof. Colin Bennett: Yes. It's not only consent, it's knowledge—knowledge and consent—and often, I think, the problem is with the first one, actually knowing and giving individuals clear, unambiguous information, not in legalistic language, about how their information is going to be used.

I actually think that the consent rules in the CSA standard are relatively clear, but I've been around this business for a long time, and the problem is really with education and implementation, and as I say, getting some clear jurisprudence on all these issues. But I'll certainly give your ideas some careful reflection.

Hon. Marlene Jennings: Thank you.

The Chair: Mr. Tilson.

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

I have a question for Mr. Rosenberg. Is it Professor or Mr.?

● (1710)

Mr. Richard Rosenberg: Professor Emeritus, actually.

Mr. David Tilson: Indeed. All right.

You raised the issue of transborder information—the Patriot Act, Canadian companies dealing in the United States going off to the FBI and other agencies, international companies operating in Canada—and where that information goes. Do you have any specific recommendations for the committee as to what the Canadian act should have on that topic?

Mr. Richard Rosenberg: That's both an important and difficult question. First of all, most people don't know that a lot of information is going off to the States. We got some publicity when the Office of the Privacy Commissioner pointed out that some of this was happening, and as I mentioned, in the B.C. context, there was lots of discussion on this when the possibilities existed that Americans could get access to the health records of British Columbians because we were outsourcing them to a subsidiary.

So they tried to put in the B.C. legislation dealing with this something to try to control to some degree the outflow. That is, if they contract out to a company, the company has to keep its records in British Columbia. At the end of the day, it wasn't clear, from either the Office of the Privacy Commissioner or the legislators, whether or not that was a foolproof way of preventing the U.S. parent company from getting access. The company within B.C., if they were going to do this thing, would have to sign agreements that they would not allow access to the Americans, they would not do this and they would not do that.

It's not clear, when you have control over information sitting in a database, whether or not it's been restricted so that the parent company can't get access. But that's the best you can do, unless you don't allow any outsourcing and it's all maintained by the government in Canada, assuming that the government doesn't outsource to companies for that purpose.

But it is a difficult process, and it will be one that's increasingly difficult, because more and more information by Canadians will go to the States by default. You'll have a credit card company; you'll make purchases. Who knows where they keep it?

Mr. David Tilson: It ended up in a dump somewhere down in the States, didn't it?

Mr. Richard Rosenberg: That also happens, yes.

Mr. Richard Rosenberg: I'm not sure exactly how to phrase this, but I guess it's a political comment. It seemed necessary, for a variety of reasons, for the B.C. government to outsource health information from the start. I would have asked if they took into account sufficiently the kinds of questions you're asking. Down the road, are you going to do this? Are you going to have to sue companies that violate? How much do you actually save at the end of the day by outsourcing it, especially by not keeping medical information in-house?

The government felt at the time that there were sufficient savings to reduce that part of the bureaucracy, and that was the way to go. I wonder indeed whether or not the questions were asked: so suppose we find violations, and how far are we willing to go to pursue recompense for those violations?

Mr. David Tilson: Do you have an opinion on that?

Mr. Richard Rosenberg: You have to go as far as you need to go. If you contract with a company and it violates the agreement by either storing it where it shouldn't be stored or allowing access that is not allowed by the law, you have to go to the limit of the law in pursuing those companies.

Mr. David Tilson: On the issue of mandatory reporting regulations on security breaches—in other words, a debit card or credit card violation is discovered—should those records be kept when they deal with and solve the fraudulent activity? Should it be mandatory that records be kept that the activity occurred, because the same thing could conceivably occur down the line years later? Do you know what I'm saying? That sort of requirement is in the United States.

● (1715)

Prof. Colin Bennett: Yes, but the American laws demand notification of consumers. Is that your question? Many of them do—they differ. If there's a security breach, the individuals affected have to be notified that this has occurred so they can take appropriate steps.

Mr. David Tilson: Yes. Then one asks the next question: should that security breach be kept on record, or is that the end of it? If you don't keep it on record, someone who is doing that fraudulent activity could conceivably do it again with the same information years later.

Prof. Colin Bennett: Who would keep it on record? I think that's the question.

Mr. David Tilson: I'm throwing that question out to you.

Prof. Colin Bennett: On my preferred solution to this issue, I know a bit about the way the American laws are not working.

Mr. David Tilson: That's one of them.

Prof. Colin Bennett: For example, I learned that in some states when a security breach occurs, the companies concerned notify the consumers and take it as an opportunity to give a marketing pitch. You know, "You've lost your data, and by the way, would you like another mortgage?"

On my preferred solution to this, the mandatory notification would be to the Privacy Commissioner, who would then make a judgment about whether the breach was significant enough for the notification of consumers to take place.

Mr. David Tilson: I have one final question.

The Chair: I'm sorry, it's seven minutes already, Mr. Tilson.

May I ask two questions please? We've heard a lot about work product. It's my understanding that work product has been defined in the B.C. legislation. Is that correct? If so, what is the definition in the B.C. legislation and how is it different from what we have?

Prof. Colin Bennett: I don't have that in front of me right now.

The Chair: Could you provide it to us?

Prof. Colin Bennett: Of course.

The Chair: Thank you.

Mr. Rosenberg, you've recommended giving the commissioner order-making powers. There's been a suggestion that we take this right out of the hands of the Office of the Privacy Commissioner and give it to some special tribunal of some kind to deal with complaints and business respondents. That would leave the Privacy Commissioner to focus on the educational aspect, systemic privacy protection, and that sort of thing.

Having made the recommendation that the Privacy Commissioner have order-making powers, are you comfortable that the Privacy Commissioner, as currently set up, is going to be able to do this under PIPEDA along with the other things she has to do under the Privacy Act? I'm asking the question of both of you. What do you think of the idea of a specialized tribunal and taking it out of the hands of the Privacy Commissioner? I'm assuming in my question that the specialized tribunal would have order-making powers.

Mr. Rosenberg.

Mr. Richard Rosenberg: I'm influenced mostly by the operations in B.C. and Alberta, where it is in the office. The office makes the orders. I see no reason why that couldn't function in Canada.

I'd be willing to listen to arguments on why a tribunal is a better way. I can see it in a way. It allows the office to focus. It doesn't get into this controversial or the continual legalistic process. But I don't see why it would not be a legitimate activity in the Privacy Commissioner's office. I know reasonable people could differ reasonably on this, but it seems to me that you need a parallel institution with as much expertise on the privacy issues as you already have in this office. Why couldn't this office's powers be extended—with additional funding, I would guess—to carry out those orders if necessary?

The Chair: Thank you.

Professor.

Prof. Colin Bennett: In my written submission that you will be receiving, I do discuss this a little bit, and I'll provide you more information about it.

The argument in favour of a tribunal is that you take the judicial function away from the Privacy Commissioner and the Privacy Commissioner maintains the ombudsman's role. You can also give it to a group of experts on the subject. This is the way the system works in the United Kingdom, and I'll give you information about how the British system works under the Information Commissioner and their Information Tribunal.

I think the Canadian Bar Association has come out in favour of such a model that is based on the Canadian Human Rights Commission and the Canadian Human Rights Tribunal. I'm not an expert on that, but I understand that it has led to delays. The perception is that it's just one other step on the way to a court, and I certainly wouldn't be in favour of establishing such a tribunal if it were of that nature. I am aware that there are arguments in the literature in favour of tribunals and that there may be a way one can be constructed in this situation, which would avoid the problems that the Canadian human rights area has. But at the moment, my preference would be some quite specific order-making powers for the Privacy Commissioner, and then an appeal to the Federal Court directly.

● (1720)

The Chair: Thank you.

Given the time, could we have some very succinct questions and short answers please?

Mr. Wallace, Madame Lavallée, and Mr. Tilson.

Mr. Mike Wallace: I have one quick question. On the order-making powers that you were just talking about, can you give me some examples of what the penalties would be and how they would be enforced? It's not just to say that you have the power, but how you're going to deal with it.

Prof. Colin Bennett: I'm not an administrative lawyer and I couldn't get into the details, but in most other jurisdictions there is a power to say, for example, "Stop doing that. Stop collecting that information." That, as we argue, typically provides the incentive to comply at an earlier stage in the process.

The role of penalties in this area of law is a tricky one, because, to a large extent, the penalties that are imposed or the penalties that are perceived by a non-compliant organization are not necessarily financial. As I said before, they are as a result of lack of reputation and bad publicity.

There are plenty of models in Canada and there are plenty of models in B.C. and Alberta—and you will receive information about those pieces of legislation as well—where there are quite precise order-making powers concerning cease-and-desist and other functions like that. Those can assist the entire investigation and ombudsman function.

Mr. Mike Wallace: Thank you.

The Chair: Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: We have only a little time left, so I will go ahead quickly.

I would like to remind you of the Wilhelmy matter in Quebec. Although our phone conversations on ordinary phones, what we call land lines, are protected, conversations on a cell phone or Blackberry are not. This led to a court injunction in 1992 in the Wilhelmy matter.

Don't you find that strange or anachronistic and that we should do something so that conversations on a cell phone or a Blackberry are protected to the same degree as conversations on ordinary lines?

[*English*]

Mr. Richard Rosenberg: Yes, there is a whole range of issues here. I've spoken in the past on this.

There is a real burden on individuals, ordinary people, to determine what level of protection their communication has. When we send a postcard, we don't expect much privacy. If we send a sealed letter, we expect privacy. If we have a telephone conversation or if we send out e-mail, what is the privacy expectation for e-mail? It's not a lot either, because e-mail bounces around in places before it reaches its destination. At every one of those places it could be determined. That's why, for people doing important business, you should consider encryption; otherwise you won't get any privacy protection.

Then you go on to these other technologies, the variation of a telephone to cell and so on. There are some real concerns about how the ordinary person determines what's protected and what isn't. You then have to lower your expectation or raise your expectation, and I think there is a real problem.

I don't see why, in principle, cellphones should be excused. Why are you making a land line...which doesn't necessarily mean a land line either, because you're sending it on a fixed line for part of the time but for a part of the time it's going over communication towers, so nothing is well defined that way. I think the simplest notion is that general forms of communication have to be protected, but there are going to be distinctions and problems in certain kinds.

The Chair: Have you any comment, Professor?

Prof. Colin Bennett: I really have nothing to say unless you want me to raise some exceptions.

[*Translation*]

The Chair: Mrs. Lavallée, do you have any other questions?

Mrs. Carole Lavallée: That's fine. Thank you.

[*English*]

The Chair: Mr. Tilson.

Mr. David Tilson: Being knowledgeable of the Alberta act and the British Columbia act, are you able to provide the committee with a list of suggested recommendations from those acts that might be applicable or should be considered here in the federal jurisdiction?

● (1725)

Prof. Colin Bennett: Yes.

Mr. David Tilson: Thank you. If you could send those to the clerk, we would appreciate that.

Prof. Colin Bennett: Yes, I said I would be presenting a more thorough submission, and I will include those.

Mr. David Tilson: Thank you very much.

Thank you, Mr. Chairman.

The Chair: Thank you.

To conclude, if I understand the presentation, Mr. Rosenberg, it's your evidence that the Quebec model has an order-making power to it. That's what you said.

Mr. Richard Rosenberg: Yes.

The Chair: I too am new to this committee, but if I understand the history, the Quebec legislation pre-dates PIPEDA. Is that correct?

Mr. Richard Rosenberg: Yes.

The Chair: Do you know, or does the professor know, why the order-making model of the Quebec legislation was rejected by the government of the day and the committee, in favour of the ombudsman type of thing? Maybe I should ask Ms. Jennings. Does anybody know the reason for that?

Professor.

Prof. Colin Bennett: There are a couple of explanations, I think. First is consistency with the federal Privacy Act and the model of implementation there. And as I mentioned, if order-making power is given on the side of PIPEDA, that would create some anomalies, but on the other hand, the Privacy Act desperately needs amendment anyway, and updating, as you may have been told.

I was persuaded by these arguments at the time, that the ombudsman model had worked very well. It was part of the culture of that office. The individuals in the office were familiar with the way that worked. I'm not here saying it has been a complete failure. There have been some advantages to it, but there have also been some clear disadvantages with respect to private sector issues and issues that do not necessarily arise in the context of government.

I gave some examples of that earlier, where the problem is not necessarily one of dispute resolution between an individual and an organization—which is the classic ombudsman approach—but one of regulation of a private entity.

The Chair: Would you go as far as Mr. Rosenberg in terms of calling on the commissioner to have order-making powers?

Prof. Colin Bennett: That's my belief, yes. The issue concerning the naming of names and the issue concerning appeal of the commissioner's orders need to be very carefully thought through. My own perception of the B.C. and Alberta models is that at the moment they're working reasonably well. But it is early days.

The Chair: All right.

Thank you very much, gentlemen. Sorry for the delay in proceeding, but I think all the members got their questions in that they wanted.

We do appreciate your time, your knowledge, and your expertise.

Committee members, this is just a reminder. On Monday afternoon we have the Privacy Commissioner herself.

This meeting is adjourned.

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

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

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