House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 033 • 2nd SESSION • 39th PARLIAMENT

EVIDENCE

Thursday, May 8, 2008

Chair

Mr. Paul Szabo

Also available on the Parliament of Canada Web Site at the following address:

http://www.parl.gc.ca

Standing Committee on Access to Information, Privacy and Ethics

Thursday, May 8, 2008

● (1535)

[*English*]

The Chair (Mr. Paul Szabo (Mississauga South, Lib.)): Good afternoon, colleagues.

Our order of the day is to continue with the Privacy Act reform. Today we have as our witness David Flaherty, professor emeritus from the University of Western Ontario, my alma mater.

Professor Flaherty has provided us with some notes that have been circulated to you. I don't think he's going to read them to us, but he is going to highlight or bring some focus to a couple of these points and maybe have some commentary on other issues or matters to which we should give some consideration as we work through this process.

Welcome, Mr. Flaherty. I appreciate your taking the time to come to share your words of wisdom with us. The floor is yours, sir.

[*Translation*]

Prof. David Flaherty (Professor Emeritus, The University of Western Ontario, As an Individual): Thank you.

I am going to start in French, but I am going to change to English because for more complicated things like the protection of personal privacy, it is easier for me to speak in English.

[*English*]

I also have jet lag. That's an additional good reason.

I feel I am almost twice as old as the Privacy Act. I started working on privacy issues as a young student from Montreal studying at Columbia University in 1964. I lobbied for the Privacy Act in the 1970s in the House of Commons during the Trudeau years and in Joe Clark's government. I've worked with every Privacy Commissioner of Canada since Inger Hansen, who was the first "sort of" commissioner under part IV of the Canadian Human Rights Act. The only one I didn't really work for was the late lamented Monsieur Radwanski. I've known them all.

I've written academic books about the Privacy Act and its origins and its development and how to implement it and things like that. I wrote case studies of data protection and privacy protection in Europe—in Sweden and Denmark and lots of countries—so I have had some comparative insights.

In 1993, through absolute good fortune, I became the first Information and Privacy Commissioner for British Columbia, which was a new position then, and I had the good fortune to move to Victoria. I was on leave from Western for six years, which was attractive, because I had the independence of returning there if I wanted to, but I fell in love with British Columbia and I've worked there since 1999.

I'm primarily a privacy and freedom of information consultant. Most of my consulting work is in the health field; in this area there are some really serious privacy issues with electronic health records and all this stuff. I have national clients. I've worked a fair bit with the federal government. I could give you as an example of a federal department that's doing pretty well at managing privacy risk Health Canada, and I take some credit for that, because as a reward for something I did for the deputy minister around 2001 I was invited to do what I call a privacy review of privacy management at Health Canada. They set up a structure, a policy department of about 35 people who advise Health Canada on privacy issues.

It's fortuitous, at least for me, that last December.... I have been an advisor to the Privacy Commissioner of Canada, Jennifer Stoddart, since she was appointed three or four years ago. I've actually known her for almost twenty years because we're both historians of Canadian law, and I published her work that far back, in the early 1980s.

Anyway, she and her colleagues invited me to do—and I emphasize this—an independent essay on the need for Privacy Act reform. I've written a 45-page essay that she mentioned to you, and that's how I got to talk with you. The essay is pretty much finished. It's fairly academic; it's tough-talking, and I'll try to reflect some of that in what I have to say to you today, but in a way you've surpassed me because you're already into the nitty-gritty of how you can improve the Privacy Act with the little things you can do and the ten quick fixes that she gave you. Mine is a more high-level overview of why this should be done.

An analogy I would use with you for the Privacy Act, which was progressive in its time, is that if you bought a house 25 years ago and did no maintenance or decoration, you'd be living in something of a slum. The Privacy Act is a somewhat slummy piece of privacy legislation. I used the word somewhere that it's risible in terms of what we need.

It reads very well in French:

[*Translation*]

the word “risible” sounds even better in French.

[*English*]

It's really a pathetic piece of legislation. I looked at it again online this morning. It was just hilarious. No wonder my federal clients aren't too bothered by the Privacy Act and its obligations: there ain't much there. There's not much meat in the sandwich. It doesn't meet the national privacy standard.

In 2000 Parliament voted PIPEDA through. I'm sure you're being driven crazy by all this alphabet soup of privacy legislation. That's the very fine piece of private sector law, the Personal Information Protection and Electronic Documents Act, which I helped lobby for in 1999-2000. It incorporates what we call the national privacy standard, which is built around ten principles.

For most of you, all you need to know is that there are ten privacy commandments, these ten privacy principles. There should be openness about what you do with personal information. There should be accountability; somebody should be in charge of the shop. You should state the purposes for which you're collecting personal information. You should limit the use, collection, and disclosure of personal information. You should get consent; I call that the adultery clause in the privacy standard, because it's the critical one. There's absolutely no consent requirement in the federal Privacy Act; it's disgraceful.

Some people say to me that the public service would never go for a consent standard. Well, why not? Why shouldn't they use either express consent, or implied consent, or notice to ask us for our personal information?

Then you're supposed to have reasonable security. There is absolutely no security requirement in the federal Privacy Act. Can you imagine that, in the years of identify theft and data breaches? That doesn't mean there's no security, but there's no standard of reasonable security against which the Privacy Commissioner can test what's actually done.

There is also the right to access your own personal information, to make privacy complaints, and so forth. That's done reasonably in the federal Privacy Act. That's about the only thing that's done well there.

I thought it was wonderful when it was enacted in 1979, 1980, 1981, and 1982. I helped push for it. But it no longer cuts the mustard, to put it quite simply. In particular, the Privacy Act doesn't begin to meet the kinds of privacy rights, constitutional rights to privacy, and statutory rights to privacy that we have under the Charter of Rights and Freedoms. It fundamentally fails to protect the privacy interests of Canadians in their relationship with the federal government.

I can tell you the story, if you wish, of the Ontario government changing the adoption law to allow individuals to have access to information about adoptees or those who were adopted, against the wishes of these individuals. Ann Cavoukian, the Ontario Information and Privacy Commissioner, fought this thing all through the legislature, etc., and she lost. But then a group of litigants led by Clayton Ruby as their lawyer went to the Supreme Court of Ontario. I was the privacy expert on a pro bono basis, and we overturned those parts of the statute, based on our articulation of privacy rights under the charter.

I would tell Canadians that over time they're going to bring constitutional challenges regarding the inadequacy of privacy protection and data protection at the federal level. And I would think that would be a good thing.

The work I did for the Privacy Commissioner's office is independent work. They're not telling me what to say. You'll be happy to know that almost everything the Privacy Commissioner of Canada and her associates have said to you makes perfect sense to me. A lot of the essay I've written seems to say “yes, sir, yes, sir, three bags full” regarding the need for educational power and various kinds of things in the ten quick fixes that Madame Stoddart has given to you. I'm completely onside with her and her colleagues. I assure you I'm very independent. There are some of them behind me, but I'm not Pinocchio, and they're not telling me what to say. They may take notes if I say something that doesn't meet the party line, but that's fine. I'm here to tell you what I think and what should be done.

The thing I'm promoting, which I think is regarded as somewhat radical but which I like very much, is the idea of giving order-making power, regulatory power to the Privacy Commissioner of Canada. I regret to tell you that it's much too easy to ignore the Privacy Commissioner of Canada. It's a talk-shop at one level. All she can do is tell you to do good or don't good, but you don't have to listen to her. I teased her yesterday. I called her a toothless tiger in some remarks I'd written. But I've changed that to a toothless watchdog, because I regard the Privacy Commissioner as the watchdog for our privacy interests, who articulates the privacy interests that are at stake in issue after issue and then helps the public bodies, helps the government institutions—and there are 250 of them subject to the Privacy Act—learn how to comply with these rules and regulations.

No doubt in the 1980s I agreed with John Grace and then with Bruce Phillips that the ombudsman role was satisfactory in just giving advice and so forth. She's not being listened to. The way you get listened to is to have the power to say “stop doing that”.

● (1540)

There was a case two years ago at the Ottawa Hospital where a poor unfortunate patient went in for open-heart surgery. When she got in there, she told them that her ex-husband and his new partner worked there. She and her ex-husband were involved in a custody dispute, and she wanted her information to be kept highly confidential. That couple, or at least the female part of it, started accessing her records right away. Eventually the ex-husband told his ex-wife that he had seen her records, knew that she was in for heart surgery, and all this stuff.

Ann Cavoukian, the Information and Privacy Commissioner of Ontario, has order-making power under both the Freedom of Information and Protection of Privacy Act in Ontario and the Personal Health Information Protection Act, PHIPA, which regulates all health information in the public and private sectors in Ontario. She issued an actual order—the situation was that bad—at the Ottawa Hospital: do this, do that, don't do something else. While this order-making power might not have to be used very often, it's a weapon or tool that can be used to bring the public service to the table to find pragmatic solutions to the issues taking place.

I will add, just while I'm thinking about it, that the public service, I regret to say, has not learned to live with the Privacy Commissioner of Canada. The last person they want to tell about their schemes and plans is the Privacy Commissioner. They wait until everything is almost finished and ready to go, a bill in Parliament for whatever it is that could be invasive of the privacy of Canadians, then they tell her about it—almost when it's too late, a fait accompli. There needs to be consultation up front with the Privacy Commissioner of Canada. There's a sorry track record of not doing that; they're not frightened of her.

I'm also arguing, in my presentation, for putting into the Privacy Act a framework for what we call “privacy risk management”. As I go from client to client on a daily and weekly basis, the way I get the attention of boards of directors, CEOs, senior executives, or in this case members of Parliament is to talk about privacy risk management. All of you know what risk management is all about, from your business backgrounds, your work in government, or whatever it is. This is privacy risk management.

We have developed some tools in the last 10 or 15 years that should be put into the Privacy Act so that every federal institution that's privacy-intensive—that is, that collects, uses, and discloses a lot of personal information—should have in place what we call “chief privacy officers”. The Bank of Montreal has a chief privacy officer, as does Aeroplan, Bell Canada, Intel, Microsoft, Oracle, Sun Microsystems, and Maximus Inc. All these companies have chief privacy officers. Why? They're a centre of privacy expertise. They're a focal point. If you put them high enough up, at the director level at least, then people will pay attention to them. They'll know to go to the privacy officer and their staff to get advice on this cross-cutting issue across the government.

The second thing they should be doing is privacy impact assessments. I helped invent, with some New Zealanders and fellow Canadians, the whole idea of privacy impact assessments. I do them regularly. They are very arcane, almost academic kinds of activities. I write them according to my own format. I'm going to send Nancy home with some background material—some of it she's seen before—on how I do these sorts of things.

The privacy impact assessments are terrific things to apply to a sensitive new database or sensitive application. They are being done under Treasury Board guidelines, but they're guidelines only. I would like to see a statutory requirement to do privacy impact assessments that are actually good ones, not lousy ones that skim over everything, and show them to and get them vetted by the Privacy Commissioner's Office, and then post them on the website so that you can actually see them. For a couple of the airline passenger information systems, I think there's a PIA on this website.

In term of privacy training, there are more than 200,000 public servants, most of whom have not had privacy training in a long time. They don't understand the ten privacy principles and wouldn't know a privacy issue if it hit them in the head. Some do, of course, but that kind of knowledge is transitory. The name of the game today is a 20-minute quiz, 30-minute test, taken once a year, with certification to your HR record that you've actually had privacy training. As I said to you before, you'll recognize that one of the basic privacy principles is involved.

There's been a lot of talk in the last few days, after the Auditor General's report, about data-sharing agreements and the lack of data-sharing agreements with the provinces for public health surveillance. That's just ridiculous. Why are they not doing them? They're a pain in the ass: you have to negotiate with the provinces, the provinces want to put the rules into the documents, and then you have to follow the rules. And guess what? The privacy commissioners from the provinces and territories might come and audit what you're doing—which they damn well should be doing.

I forgot to mention earlier that my argument for order-making power is largely derived from the fact that in Quebec, Ontario, British Columbia, and Alberta, which have pretty decent pieces of privacy legislation, the commissioner had order-making power. I used to get the attention of the British Columbia government, the NDP government of Glen Clark and others, in the 1990s. You can imagine what fun it was to be a privacy commissioner then. Life was pretty good because of the privacy impact assessments and the fact that I could get their attention because I could order them to do something.

● (1545)

I also want to leave with you this idea: the Privacy Act and PIPEDA were the products of political leadership and leadership in the public service. It was Perrin Beatty who brought the first Privacy Act, in a private member's bill in 1980, before the House of Commons. Then Francis Fox, from another party, with the Trudeau government coming in, put through the Access to Information Act and the Privacy Act. That was political leadership. In the 1990s we needed to regulate the private sector, and it was Allan Rock, justice minister, and John Manley, industry minister, who stepped up to the plate and said yes, we should be doing this.

If there's anything you can do.... In my opinion, the heavy lifting here has to be done by the Department of Justice.

I forgot to tell you that twenty years ago they had this report—*Open and Shut*, for 1984 to 1987—on how lousy the Privacy Act was and how it needed to be improved. Guess who was the expert on privacy for three years? Me. What did we get out of it under the Mulroney government? Nothing. Nothing was done. Some policy changes were done.

All the recommendations we made twenty years ago are still relevant, but what has happened in between? The Internet, the World Wide Web, ubiquitous computing—imagine trying to use the old Privacy Act to control that kind of stuff.

The political leadership also came from people I call “policy entrepreneurs”. In the 1970s there were three or four senior public servants—Barry Strayer, now in the Federal Court; Gill Wallace, subsequently Deputy Attorney General of British Columbia; and I've forgotten the other names—who recognized that it was part of an international movement to have sound privacy management in the federal government. That then was replicated in Ontario and Quebec. Quebec was actually the first, even before the federal government, in 1981, as I recall. I gather you're having Paul-André Comeau, one of my former colleagues as Privacy Commissioner, to talk to you before too long. He knows the Quebec scene much better than I do.

I think you also as politicians—this is my final point, at least in this beginning presentation—have to ask why doesn't the federal government, why doesn't the bureaucracy, why don't deputy ministers want a stronger Privacy Act? It would be a pain in the ass. They'd have to do things much more carefully than they're doing them now. Their power would be constrained. They wouldn't be able to have kind of a free-for-all with the personal information of Canadians.

They have a lot on their plate, I will admit. There are a lot of other issues they have to deal with. But the Privacy Act, like the Access to Information Act, is cross-cutting. Everywhere in the federal government there's personal information collected, used, disclosed, retained for all kinds of purposes for very long periods of time in more and more massive databases and with more and more data-sharing across government institutions.

I have no objection to outsourcing. I'd be happy to discuss the outsourcing in B.C. with you. It's in my speaking notes. I have no objection to data-sharing with consent. If I want to file my tax return online, I'm doing it consensually. That's exactly the way it should be. All of our relationships with the federal government should be based, to the fullest extent possible, on consent.

In 1999-2000, when PIPEDA was going through, I was lobbying on behalf of Industry Canada as a paid consultant. The Canadian pharmacy association said that we were going to shut down pharmacies in this country if we put PIPEDA through. Why? Because every time someone came in with a prescription, the pharmacies would have to read people's privacy rights to them. We told them that was crazy; we'd be using implied consent.

When I take a prescription to my druggist and hand it to him, why do you think I'm handing it to him? Is it just so he can have a little read? No; it's to fill my prescription. So I'm giving implied consent, as you do, to use my personal information for the purpose of filling a prescription. But then if he starts calling me up and saying, “I see you have this little medical problem, and I have this hot new product I'm selling on the side”, I'd be quick to complain to the Privacy Commissioner. That's a completely unacceptable use of my personal information. It's not in the statement of purposes for which the personal information is collected.

I hope those introductory remarks, plus the 30 other points I've made in my written stuff, will whet your appetite. I'm a teacher by background, so I'd be particularly happy to help you understand some of this stuff. There's no particular reason, as lay persons, you should have gotten a university degree in Privacy 301.

Thank you.

● (1550)

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

We're going to move quickly to questions.

Mr. Dhaliwal, please, seven minutes.

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

Thank you, Mr. Flaherty, for coming here. I also congratulate you for the lifelong work you have put into the privacy legislation. I'm certain we can benefit from your experience here.

You commented on the bureaucracy when you were talking about privacy legislation. Where is the challenge in improving Canadian privacy? Is it in improving the laws or the policies? Is it in the implementation of these policies? Or is it the bottleneck?

Prof. David Flaherty: When you're doing the privacy risk management strategy, the first thing you have to have is a law.

When they first introduced the freedom of information law in Ontario, my comment to the media around 1983 or 1984 was that I thought any law was better than no law until I saw this law. It was pathetic, so it was never introduced. Ian Scott, as Attorney General, actually took the initiative and went into his own law office, when he became Attorney General, and drafted the bloody thing. It's the model we use now in Alberta and British Columbia. It just shows what leadership can do. So if you don't have a good law, you have a problem.

Schedule 1 to PIPEDA, which is the Canadian Standards Association model privacy code, is where you find the ten privacy commandments. They were a product of the public sector and the private sector in the mid-1990s. Smart characters like me said, “This is a wonderful code. Why don't we give it the force of law?” They give it the force of law in PIPEDA. It was like putting the ten commandments into law in one way or another.

If you don't have a good law, you have a problem, but then you need a privacy policy. Then you need chief privacy officers, a privacy team, meaningful confidentiality agreements, frequently asked questions on websites for the general public, and privacy impact assessments to make the system work.

I'm not sure I've totally answered you. I started a filibuster already, and it's only the first question.

Mr. Sukh Dhaliwal: You have done work in B.C., and you have praised the work that the Government of B.C., along with you, has done. Could you explain what the B.C. government has done to modernize its privacy laws?

Prof. David Flaherty: If my successor, David Loukidelis, who appeared before you on PIPEDA last year, were here—and of course he told me what to say when I was here, so I have to remember all the things he told me to say, not particularly on this question—he would be talking about the need for the British Columbia government to appoint a chief privacy officer. I recently advised a major university in British Columbia to appoint a chief privacy officer. I'm working for two crown corporations there at the moment, and they need a chief privacy officer.

The B.C. law is from 1993. It's not too antiquated. It's not adequate for an electronic health record environment, and we still need more resourcing of privacy management by the B.C. government.

They have chief information officers. They should have chief privacy officers to go along with them, and then the two of them would work together, because you have to marry privacy and security. There are all kinds of resources in security, and too often there are not enough on the privacy side.

I wouldn't run around claiming that the B.C. government is doing A+ work on the privacy field. When these new laws are brought in, there's a honeymoon phase, like any other honeymoon, and then resourcing goes down; interest goes down; privacy training goes down; and people like new commissioners have to come in and give the whole system a kick-start, which is more or less, after a lengthy hiatus of 25 years, where you are with this crummy privacy act.

● (1555)

Mr. Sukh Dhaliwal: Your study, when we look at it, is also based on other countries like Germany, Sweden, France, and the United States. Could you discuss the privacy innovations in those countries compared to ours here?

Prof. David Flaherty: You don't want to do anything in the way of European data protection. It's so complicated. It's so rule-bound. It's inspired by the European directive. It's very legalistic. It deals primarily with law rather than practice.

My interest is in policy. What happens in practice? In the privacy game, the motto is say what you do, as an organization, and then do what you say. Whether you're running an auto dealership, a drugstore, or Health Canada, say what you do with personal information, and then follow it up with compliance. I've written about these European countries. My knowledge is not as *au courant* as it was when I was writing books and when I published in 1989 my big book on the five countries. That's where I learned how to do it—by watching what they were doing.

I don't think there's much to be learned from the continental European countries. In my paper I talk a lot about the fact that the ultimate goal here is robust privacy protection and robust security so that we keep ourselves from living in surveillance societies. My book in 1989 was *Protecting Privacy in Surveillance Societies*. People thought I was writing about the Soviet Union, mainland China, or something like that. In fact, I was writing about Germany, France, Sweden, the United States, and Canada. Most of us believe that the United Kingdom, in particular, is the worst example in the English-speaking world of a surveillance society, where you're being watched all the time. Public health surveillance, cancer cohorts, and that kind of thing—those are examples of good surveillance. Then there's bad surveillance.

There was a lovely editorial yesterday in the *National Post*. It was called "A bad day for Big Brother". Some student or researcher in the United Kingdom had stood up and said, you know, we have the most massive investment in surveillance cameras in the entire world. We're being watched all the time. Most of the time the cameras aren't working. They're no good in preventing crime. They're too grainy to actually see anything, and it bores the hell out of people to watch them. That's the kind of country I don't want to be in. I don't want to be watched all the time. I couldn't imagine why you'd have a surveillance camera on me. If you were videotaping, that would be fine, with my consent.

The ultimate goal is to keep from being watched all the time for bad things. If we're all suspected terrorists, I want to be watched until I'm blue in the face. If it's a law enforcement matter, we can balance the privacy rights of individuals and law enforcement and national security. I think the Privacy Commissioner knows a lot more about national security, in particular, than I do. It's not as if, you see, we privacy advocates want to trump law enforcement or dealing with child pornography or whatever the other evils of society are. We simply want to know in advance what the rules are going to be and how the personal information is going to be used.

I got along famously with the deputy chief of the Vancouver Police Department and with the Victoria police, as well. They had their job to do, and I watched what they were doing. When they had books of known prostitutes sitting around on open desks, I'd say, you know, do you really have to keep that where people can see it, or can you come to a slightly more sophisticated data gathering system? Any time anybody calls 911, how long are you going to keep that information?

Data retention and data destruction are good things. I have clients who have kept records for fifty years. They've never destroyed anything. Why?

The Chair: Okay.

We're going to move on to Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): It is a shame to interrupt you while you are on such a roll, but I have questions for you too, Professor Flaherty.

First, I would like to thank you for your document; I read it carefully. I was astonished at some of your more, shall we say, unique passages. You said that the current act is almost useless and even risible in the 21st century.

● (1600)

Prof. David Flaherty: I like words.

Mrs. Carole Lavallée: I like words too, which is why I like to use them correctly. I do not think we can go that far. You wrote it more to grab our attention than because you believe it. After all, the present wording of the act protects some of our information. Anyway, I will not take up all my discussion time talking about your skills and your literary style.

I would like to go back to the commissioner's ten recommendations. You said that you are in close contact with her and that you are of like mind in some respects. You have studied the commissioner's ten recommendations. Are there any that you do not agree with?

Prof. David Flaherty: No, but when I read them this morning, I marked recommendations 1 to 4 and 9, because I found them more substantial than recommendations 5 to 8.

Mrs. Carole Lavallée: I want to make sure that we have the same numbers. The tenth recommendation deals with cross-border information sharing. Are you saying that this recommendation is not one of your priorities?

[*English*]

Prof. David Flaherty: I'm a little tired of transported data flows, because the *Open and Shut* report in 1987 recommended that we should really be studying transported data flows of personal information, and nothing much was done about it. They commissioned a study, which I didn't get to do. A bunch of scholars at UQAM, Université du Québec à Montréal, did it, and nothing happened legislatively.

I gave a talk about electronic health records in Vancouver on Tuesday afternoon. I was talking about the U.S.A. Patriot Act and what it costs the taxpayers of British Columbia to comply with the special laws that were brought in in British Columbia because of Patriot Act concerns. Contracts that had already existed were grandfathered.

The credit bureau of Equifax, the credit reporting company, to the best of my understanding is in Atlanta. My Visa card every month is processed in Atlanta, and the Privacy Commissioner said that was okay. We actually have massive flows of personal data that we've approved of, that we think make sense. Some of it's now going to India and is being outsourced and all this kind of stuff.

My point is that we have to know what these data flows are. I point out in my paper that I was an advisor to the commissioner on her audit of the Canada Border Services Agency and of the flow of information on us across the border to the Americans. I have a PhD in American history. I taught it for many years. I'm not vaguely anti-American, so that's not where I'm going with this, but we simply can't be handing over our personal information across the border to the Americans without data-sharing agreements about how it's going to be used and for what purposes.

We need a record of what's happening, and that doesn't exist at the moment. The commissioner said her power was limited by the border. The Canada Border Services Agency, if it's going to engage in data exchanges back and forth across the border, should know what they're doing.

Mr. Dhaliwal mentioned the United States. No country in the world has more privacy law than the United States, but nobody has a collection of more meaningless privacy laws than the United States. That's only a small exaggeration. There's no enforcement except in the courts. There's no privacy commissioner in almost any of the American states or federally. The Federal Trade Commission is doing some useful work in consumer rights.

The American model is highly decentralized, very court-driven, very expensive, very difficult to influence. Our data's going over there. We don't know what's happening with it, and nobody's minding the shop. I certainly don't think the director or the president or whatever he is called of Homeland Security is a good custodian of my personal information when he doesn't even think fingerprints are sensitive personal information.

[*Translation*]

Mrs. Carole Lavallée: I still do not understand. Are you in favour of recommendation 10?

Prof. David Flaherty: Yes.

Mrs. Carole Lavallée: You are in favour.

Prof. David Flaherty: But it is not just a matter of saying yes, is it?

Mrs. Carole Lavallée: I could understand *yes*.

Prof. David Flaherty: I agree with all ten recommendations.

Mrs. Carole Lavallée: But you do not think that there are enough of them.

Prof. David Flaherty: Pardon?

Mrs. Carole Lavallée: You think that there should be more.

Prof. David Flaherty: Yes.

Mrs. Carole Lavallée: I would like to go back to the order-making power that you would like the commissioner to have. You know that she does not want that power. You are not of like mind there. You are not in agreement. You say that she needs order-making power because, without it, no one takes her seriously. I have difficulty understanding why the commissioner does not want people to take her seriously.

[*English*]

Prof. David Flaherty: It's too easy to not let the Privacy Commissioner know what's going on.

I'm being oratorical to make points, and I'm exaggerating a little bit to make points. It's not as if nobody listens to the Privacy Commissioner of Canada, but think of how many times she's done major reports—in June 2006 in particular—on reform of the Privacy Act, and the Ministry of Justice has done nothing. The most important audience, as far as I'm concerned, is Rob Nicholson, the Minister of Justice, who should tell the damn deputy to go do something.

You know the concept of being trapped by a paradigm or a certain way of thinking or a world view. We're all victims of that in any particular time period. There have been 25 years of the Privacy Commissioner's office. Some of the people sitting here have been there since the beginning in 1982. It's difficult to break out of a mindset that you're accustomed to.

My great friend Bruce Phillips would throw glasses at me for arguing that the Privacy Commissioner should have order-making power, because he thinks he could do it by just jawboning or talking. I don't think that's enough in 2008 or going forward.

I said to you somewhere that I'm not a futurist because I'm an historian. I don't know what kind of a privacy act you need for the next 25 years, but.... Sorry.

● (1605)

[*Translation*]

Mrs. Carole Lavallée: I am the one who is sorry because my time is up and yours is not.

[*English*]

Prof. David Flaherty: My point is you have to be looking forward, not backwards, as to what you need, and that's where the order-making power is very significant.

The Chair: I might just suggest members might want to manage the witness a little themselves too.

Mr. Tilson.

Mr. David Tilson (Dufferin—Caledon, CPC): I'd like to talk about the order-making power.

First of all, I want to say I think we're all impressed with some of your qualifications, and that you have come to provide comments to us. I think you must live, breathe, eat, and sleep privacy. Good for you.

Prof. David Flaherty: I was dreaming about this morning's appearance. Maybe it was a nightmare, and I didn't record it properly.

Mr. David Tilson: Yes.

The commissioner has indicated in the past that she believes she should have order-making powers. I suspect you do too, because you are on her advisory committee, and you've known her for years. I understand that.

You were the first Privacy Commissioner in British Columbia, and between 1993 and 1999 you made 320 orders. I would be interested in knowing what percentage of those were on privacy and what percentage were on information.

Prof. David Flaherty: Almost all of them were Freedom of Information Act decisions, but many of them had a privacy component. I'm giving you a lot of information in a relatively big hurry.

The power I had was to issue an order to stop doing this with personal information or start doing something with personal information. For example, I discovered when I went on a site visit, an audit, that B.C. Hydro was using social insurance numbers in 1994 to keep track of their clients and send out bills, and I said, "Stop that. You can't do that." So they stopped it. I didn't have to issue orders or anything like that.

Mr. David Tilson: That's okay.

I guess what I'm getting at is that I think we decided some time ago that having privacy and information under the same commissioner would be inappropriate. We've made that decision, and that's the end of that.

Has commissioner David Loukidelis made a similar number of decisions, and have those mainly been with respect to information?

Prof. David Flaherty: Most of the privacy stuff is settled through investigations, complaints, audits, and site visits. I thought you were going to talk about judicial review.

Mr. David Tilson: I'm coming to that. I'm just laying the groundwork.

Prof. David Flaherty: Good.

Mr. David Tilson: Obviously, then, one looks at mediation. We look at investigation. We look at investigators trying to talk and people making inquiries. Maybe there is some other way of doing things, whatever the mediation process is. That's all fine and good.

The commissioner educates the public; the commissioner educates us. The commissioner advises Parliament, advises us, advises members of the public, has education programs, provides lectures across the country, sets up a website, makes investigations. And there are probably other things I can't think of.

So the question I'm getting at is if she gets order-making powers, will she have some sort of conflict? I'm not talking about mediation; I'm talking about someone who would actually hear the evidence and make orders. That person would have to have a fair bit of academic training and perhaps some legal training. We're setting up a quasi-judicial board. My question is whether there would be some sort of conflict.

● (1610)

Prof. David Flaherty: I was asked the same kind of question by the former NDP member Dave Barrett, when I first met him in 1994 or 1995 and he had just published his memoirs. Every so often people certainly ask if there is a conflict in being the Freedom of Information Commissioner and the Privacy Commissioner. There isn't. One deals with general information, and the other deals with identifiable personal information.

I am not prepared to talk with you critically about how the current Privacy Commissioner or her predecessors do their work. Some of the work of those offices has become much too legalistic. On the freedom of information side, really, if you're issuing orders, you have to be quite legalistic.

If you look at the investigation reports of all sorts of things that I wrote and my successor wrote, that the Quebec commission has prepared, that Ann Cavoukian has done, on things such as the case at the Ottawa Hospital—she actually issued an order, but it was basically a story that said here's what happened in the Ottawa Hospital—there are all kinds of these things on the website, and there is always a legal staff involved.

The good thing is—and I want to make sure I say this—that even if the commissioner had order-making power, it would be subject to review in the courts, and it wouldn't be an order-making power on everything. Right now she has only too limited a way to get to the courts, as she has explained to you quite nicely. She can only go to Federal Court for a couple of small things. She should at least be able to go to court on a much broader range of things, and get the courts into the game.

Mr. David Tilson: I understand all that. I don't know about the other caucuses, but I don't think ours has actually formed an opinion yet as to where we stand on this order-making power. Personally, I understand some of the arguments that have been made. I look at the cost of it. I mean, my goodness, we can't....

She was here some time ago. She doesn't even have the staff to complete the backlog she has now. It would take an enormous amount of money to set up lawyers, advisers, people who push paper. It would be incredible. She doesn't have the resources to do what she's doing now.

Prof. David Flaherty: That's because you're making her, under the current Privacy Act, pursue so many complaints that are almost useless. That's why she wants to get out of having to investigate every complaint.

I think it's scandalous that it takes a year to get a privacy complaint investigated. It's difficult for your constituents. It's unacceptable. But so many of the complaints are the same darn thing over and over again.

I was much more interested in going out to hospitals and prisons, seeing what was going on, and doing investigations. I did a site review of the B.C. Cancer Agency and found all kinds of things. We went back a second year and got them all fixed up. And I had 25 staff.

Mr. David Tilson: Don't investigators now do a form of mediation? Isn't that what they're doing?

Prof. David Flaherty: Yes, but it appears to go very slowly because they can't say that someone is what I call the "frequent flyer". I had 100 cases with one character. It was ridiculous. I tried to put him in the penalty box. I did for two or three years. The courts said I could only put him in the penalty box for a year.

Mr. David Tilson: You know what; I may change my mind on this, but quite frankly, I think if we give her order-making powers the whole process will come to a dead stop. Someone may change my mind on this, but from listening to what you said and listening to what she said about how she can't do her job now, if we had all this other.... This would be massive. I believe it would come to a dead stop, the whole process.

Prof. David Flaherty: That's a credible position. Remember, there are 217,000 public servants; there are 140 staff at the Privacy Commissioner's office. There are 86,000 people at Canada Post who are all supposed to be complying with the Privacy Act.

Mr. David Tilson: There you go.

The Chair: The committee certainly is going to pursue that whole discussion once we hear from the rest of the witnesses.

Mr. Pearson, you have five minutes.

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

Welcome, Professor. It's nice to have you with us today.

I'd like to ask you about privacy impact assessments, but before I do, I think Mr. Tilson was on a good line of questioning.

You talked about the Ontario Privacy Commissioner. I would like to know if there are any limitations on her powers.

Prof. David Flaherty: Yes, definitely.

Mr. Glen Pearson: Could you explain what those are?

Prof. David Flaherty: When I circulated my paper to the Ontario commissioner, to my friends.... I know all these commissioners. I work with them. I do consulting work for them. They employ me to do things. In fact, I think the Privacy Commissioner can and should use more consultants and law firms to help her when she has huge backlogs. There are lots of people with privacy expertise in these places, and consultants.

How's that for a self-interested statement? I already do work for these various commissioners.

At any rate, she has a staff of about 100 or 120. It's a big operation. She has the entire health sector, the municipalities, and the provincial government in Ontario. She's a leader in very many ways on critical issues, such as RFIDs, biometric encryption, and all this stuff.

Under PHIPA she has much broader order-making power. What happens is that the later the law, the better and the more power there is to it. PHIPA, the Personal Health Information Protection Act, was enacted in 2004. You'll be amused to know that it's 120 pages long, and the non-legal guide to it is 800 pages long. I might try to tell you all this stuff is pretty simple, but it's simple at the ten privacy commandments stuff; it gets more complicated when you apply it in practice.

Her job is to apply these rules in a sophisticated way by doing investigations and things like that....

As I said, I have a bit of jet lag. I've lost track of what you actually asked me.

● (1615)

Mr. Glen Pearson: That's fine, I understand.

She doesn't have limitless powers.

Prof. David Flaherty: It's not unlimited power, no.

You have to remember that a parliament, a legislature, a government can do whatever they want. I opposed PharmaNet in British Columbia. Glen Clark and his government did it. That's perfectly acceptable. No one is trying to make these privacy watchdogs have absolute power of any sort. But I want them listened to. That's the strongest argument I have. In the federal government, the Privacy Commissioner's office is not being adequately listened to. I know that because I do consulting work for these organizations. I know what's going on. And it's not good from a privacy protection point of view.

Mr. Glen Pearson: Thank you.

I'm still trying to get my head around privacy impact assessments, especially in light of what the Privacy Commissioner told us. Can you tell me how they currently work? And can you add whether you think the policy for that should be legislated?

Prof. David Flaherty: Yes, I definitely think the policy should be legislated, but I don't want a whole bunch of cookie-cutter PIAs every time they change the personal information system. Any significant personal information system at Health Canada or Service Canada or Revenue Canada—whatever they're called nowadays—should have a privacy impact assessment done so that Canadians who are interested can go to the website and find out, "Oh, this is what they do with my personal information."

My favourite client is the Canadian Institute for Health Information. They have 18 major databases. They're kind of the Statistics Canada for health, as you likely know. They have 18 privacy impact assessments on their website, www.CIHI.ca, under privacy and data protection. I wrote the first drafts of each of them with the staff. One is about therapeutic abortions. CIHI has a therapeutic abortion database? Yes, it does. Does it have identifiable data? No. Does it have very strong security provisions? Is it audited? Is it monitored? Yes. Does it exist for good purposes? Yes. And if you don't think it exists for good purposes, you can fight with them.

The PIA is the story of a database. Why does it exist? What are its purposes? Why do you need this in the first place? Is it rational? What personal information do you collect? What personal information do you disclose? Do you get consent? What security provisions do you have in place?

I always end up with a privacy report card, measuring the thing against the ten privacy principles. I've done it for the Assembly of First Nations regional health survey, which is in the field at the moment. I sometimes give actual grades to it—for example, 72% on security, 85% for consent or accountability.

Mr. Glen Pearson: Mr. Chair, do I have any more time?

The Chair: You have one minute.

Mr. Glen Pearson: Just to follow up on what Mr. Tilson was saying, you were talking about the Privacy Commissioner. Part of the problem she has is that she has such a backlog, she ends up investigating things that are useless to do. How does the Ontario Privacy Commissioner triage or prioritize those things?

Prof. David Flaherty: I don't know why they're getting so many complaints federally. I think I read in the last 24 hours, or somebody told me, that 50% of the complaints are from Corrections Canada. Is that right?

Anyway, it's a huge number. I was laughing to myself, as I was thinking about this, that it's a good thing....

Pardon me?

Mr. Rick Norlock (Northumberland—Quinte West, CPC): Actually it's more.

Mr. Glen Pearson: But how does Ontario prioritize?

Prof. David Flaherty: In British Columbia we can ignore requests and say they're frivolous and vexatious. I think that's what the language is.

What I learned in 1993, when I finally ran something, having been a professor all my life, was that a lot of people have various things happen to them that they want to change. They go to the ombudsman, they go to the Auditor General, they go to the Privacy Commissioner, and so on. They somehow think they can change the facts of what happened. It's like a circus.

Mr. Glen Pearson: Thank you.

The Chair: Monsieur Nadeau, *s'il vous plaît.*

[*Translation*]

Mr. Richard Nadeau (Gatineau, BQ): Thank you, Mr. Chair.

Good afternoon, Professor Flaherty. In the documents that you provided to us...The present commissioner made ten recommendations. The act should have been amended a long time ago to bring it up to date rather than leaving it as a kind of artifact.

What are the critical amendments?

● (1620)

Prof. David Flaherty: Critical?

Mr. Richard Nadeau: Critical, urgent.

[*English*]

Prof. David Flaherty: Very, very important?

Mr. Richard Nadeau: Like, they need to be done now.

Prof. David Flaherty: Okay.

I'm extremely reluctant to recommend to you that you throw this issue to justice department lawyers and policy analysts for serious study, because it could be five or ten years before something happens. You have to ask yourself why nothing has happened for all these years. Partly they fight among themselves at the Department of Justice, etc.

I appreciate the fact that Madam Stoddart, for whom I have the greatest admiration, and her staff have a lot of burdens. They're doing as well as they can under the circumstances. I think her idea of ten quick fixes for you is a good thing. I have trouble imagining that you're going to have the resources in the next couple of months to redo the Privacy Act by yourselves.

I think the most important thing is to, through your caucus of the government, persuade Mr. Nicholson to do something. It doesn't have to be done in two weeks, but really, some things have to be done seriously and as quickly as possible. I believe it shouldn't be just one caucus. This is the kind of issue that's cross-cutting. It's not a small-l liberal or a big-L Liberal or small-c conservative issue. It's not an NDP issue or a Bloc Québécois issue or whatever. It's for all Canadians, all residents of the country, all privacy interests. And it's your privacy interests as much as mine, and your constituents'.

So I'll take anything I can get. If ten quick fixes is what you can do reasonably, then do it. I hope you will give, as they say in French, *les grandes lignes*. I hope your committee will give *les grandes lignes* to the public servants and to Kevin Lynch. Kevin Lynch, who was responsible for PIPEDA, as the Deputy Minister of Industry Canada, understands these things. I lobbied him myself in the mid-1990s, when I was the privacy commissioner over in Oxford, that PIPEDA was worth doing. He would remember that. We walked for a couple of hours and he asked at least as difficult questions as you're asking me today: why should we do all this stuff, why should we regulate the private sector? And you should build on that.

We regulated the private sector. There were all kinds of howls. People didn't like it. Is Aeroplan in front of you, or Air Canada, or Bell Canada, or Air Miles, saying they want you to get rid of this legislation? No. They've learned to live with it. Why? Because they systematically implemented it. They know how to make something work in the private sector. We have to get the same things in place in the public sector.

[*Translation*]

Mr. Richard Nadeau: Quebec, Ontario and British Columbia, and others, have laws governing personal information. You say that the commissioners there have more teeth, more clout. We cannot say the same at federal level.

Is this because it is bigger, or because there is a lack of political will?

[*English*]

Prof. David Flaherty: There was great enthusiasm in the 1970s and 1980s for the concept of the ombudsman and ombudsman powers. It was reason together, conciliate, moderate—all a great idea. You could argue that for the level of privacy issues we had in the 1980s, the Privacy Act was sufficient, but we're now in the World Wide Web in which you're using cell phones, and you're sending e-mails, and you have no idea where the information is. You have no idea where your data is being stored.

Growth in Facebook is exponential. I bring to your attention the case of somebody who informed her friends in England a week or two ago on Facebook that she was leaving her husband. He murdered her. There are risks of using even something like Facebook, and the various commissioners have done good work on that.

We all know, from the way our own lives have changed with the BlackBerry and computers and terminals and automation, how dramatic the change has been, and we don't even know some of the risks involved for our children, and things like that.

What I really would like to talk about sometime is health and the electronic health record. Once you build a big database of electronic health records without robust data protection and privacy and security in place, then you're really in trouble, because if there's a big database, somebody is browsing the database. We have lots of reports in the privacy community, from my successor in B.C., about people who just like to go into databases and abuse personal information. There has been lots of theft by the Mafia and gangs in Quebec from various databases of the government. That's another reason we have to have really good security, really good auditing. I want machines watching machines. We can do that if the will is there, but the public service has to be told to do it and make it work efficiently.

● (1625)

The Chair: Mr. Norlock.

Mr. Rick Norlock: Thank you very much, Mr. Flaherty, for coming in. It is quite obvious that you are probably one of the most knowledgeable persons in this country when it comes to the Privacy Act.

Prof. David Flaherty: I should get a life, right?

Mr. Rick Norlock: No, because that's how we learn from each other.

I always like to hear from somebody like you and then from your nemesis, somebody who thinks on the other side of the issue. Quite frankly, I get as angry as hell when I think that someone might use my personal information for something other than what I intended it for, and I do want there to be sufficient legislation to protect me from people like that. If the legislation doesn't, then I'll do it myself, and I'll sue the bugger.

One of my tremendous worries, and one of the reasons I got involved in government, is my tremendous fear that by trying to have the government do everything for us, we create a huge bureaucracy, the very bureaucracy that you, as a privacy commissioner, sometimes fought against. We develop huge bureaucracies in every single place, which actually don't speed anything up. They slow things down. I'm not saying that a privacy commissioner should have only 50 people working for him or her, but when I hear you say something like “My God, there are 217,000 civil servants. There are 84,000 people at Canada Post. We have to watch those guys, and you have to give me sufficient resources to do it, and every law and regulation that they pass has to be filtered through us to make sure that it...”, I ask how many people you are talking about.

You had the job before in another province, and you advise the current commissioner on certain things that she needs you to advise her on so she can get things done. You have the ten commandments. I've heard what you had to say. It's obvious to me that you have a pretty darned good idea of how many people it would take for a Privacy Commissioner, under the right kind of legislation in Canada.

In five sentences or less, can you tell me how many people that would be?

Prof. David Flaherty: If you built privacy risk management into federal government institutions, all 250 of them that are subject to the Privacy Act, the Privacy Commissioner's job would be a lot easier. That's what I'm looking for. Rather than doing original work, she'd be saying "Come and tell me what wonderful things you are doing". It would be a privacy check-off at cabinet before anything came forward. Members of Parliament and committee would ask if you had talked to the Privacy Commissioner. That's what we need.

I'm as anti-bureaucratic as you are. It drives me crazy when I see the numbers of people it takes to do things.

Mr. Rick Norlock: Thank you. And by the way, I'm not really anti-bureaucratic. I think we need a bureaucracy to run things, but we don't need a system that says the more people you have working under you, the more money we're going to pay you. Everybody is building that empire. That's what we have, and I know that because I worked for the Ontario civil service, and I saw it in my little corner of the creek.

I want to understand, because I think you and I may think very much alike, how we protect an effective, efficient civil service, or bureaucracy, since it all means the same thing. How do we protect ourselves from someone, let's say in finance or health, who says okay, we have this new law that Mr. Flaherty and the commissioner want and now we're going to need somebody who goes over and consults with them, so we're going to have to create this whole new body and have deputies? How do we make sure that although we might not grow the Privacy Commissioner's group of people, that everybody else who has to report to her now is not going to have to have 15 or 20 people working for them to consult with the Privacy Commissioner?

Prof. David Flaherty: The Privacy Commissioner pointed out to you that every public servant above a certain level has to have human resources and finance training. Do they need privacy training? How do you create a culture of privacy, a culture of concern and awareness of privacy? Who are the champions of privacy in federal government institutions? It's not the deputy minister most of the time. Who is it?

You need privacy champions in place. I'm thinking about what you said about bureaucracy. Homeland Security revealed in the last couple of days that air marshals are being bumped off flights they are supposed to be on because they are on a no-fly list. I just shake my head. That's something we've just been reading about.

When I hear the Department of Homeland Security guy, who sat in front of me and spoke at the privacy commissioners' big international conference, asking why I'm worried about fingerprints, since they're not personal information and you leave them behind as you go around the world, I just shake my head. And he parades around as a bit of a privacy advocate.

I heard his chief privacy officer speak at a big security conference in Victoria in February. It was the most useless stuff I've ever heard. It was totally vacuous.

● (1630)

Mr. Rick Norlock: You're not telling me what—

Prof. David Flaherty: I'm venting.

Mr. Rick Norlock: Yes, but you're valuable. That's why you're here, and I can appreciate you've got some problems with—

Prof. David Flaherty: Homeland Security. I'm using that as an illustration of bureaucracy.

Mr. Rick Norlock: I have to remember that. I was going to use the "Y" word, but I mean our friends to the south of us—

The Chair: Time's up.

Mr. Rick Norlock: I'd just like to know how we can create that lean, mean, and effective civil service.

The Chair: We'll take it off Mr. Van Kesteren's time.

Okay, that's good.

Mr. Dhaliwal, go ahead, please.

Mr. Sukh Dhaliwal: Mr. Flaherty, I also have problems with security agencies when I see a respected member of Parliament being on the no-fly list when that member had nothing to do with any terrorism. I'm going to stay away from this.

Mr. David Tilson: Are you pointing at me?

Mr. Sukh Dhaliwal: No, it was not you. It was one of the other Conservatives.

In her recommendation the Privacy Commissioner said she would like a "necessity test" in the legisltion for the collection of personal information. Could you comment on the current use of this test, where it has been implemented in Canada or elsewhere? Has it proven to be cumbersome, or is it manageable?

Prof. David Flaherty: You may think I'm going around in circles again, but whenever I fill out a form for an insurance claim, at the bottom it says "You hereby authorize us to send all information" to whoever the hell they want to send it to. I always strike it out and say "all relevant information".

There are several principles we privacy types are pushing. I want to emphasize that I'm a privacy pragmatist; I'm not a privacy fundamentalist. But I do care about privacy. Those are nice distinctions.

Under the “necessity” principle and the principle of data minimization, you should be collecting personal information only because you need it. It's much too easy to fill out a form. There could be 40 boxes on an electronic form, and the thought is to fill them all out because the information may be needed some day in the future.

If there is a reason for it, I have no problem with someone collecting it. We always watch, for example, people collecting information. Imagine if you went to rent a car and someone had a form at Avis asking for your sexual preference. Huh? Duh.... I see forms collecting information on the religion of lottery winners. What does that have to do with it? Are people going to be smart enough to say, “You can't ask me that. Give me my $10,000 or million dollars”?

This is the kind of stuff that's going on. So we have to put in a “necessity” principle. We have to minimize data collection. We should have to give out as little personal information as possible to do the job when we fill out a form electronically or on paper. When you see things that are asking for a social insurance number, why do they need that?

Mr. Sukh Dhaliwal: As you mentioned in your presentation, you are concerned about the privacy rights of all Canadians—as are we, which is why we're studying this particular topic. You say that the Minister of Justice must make reform of the Privacy Act a very high priority. In your opinion, what would it take for him to make it high priority, and what steps should we be taking?

Prof. David Flaherty: I think you really know better than I do. I'm given to understand....

Mr. Nicholson sat through three years of hearings on the Privacy Act, from 1984 to 1987. He signed on to the *Open and Shut* report, and he knows that the Mulroney government did nothing, in part because they hated the Access to Information Act. The great heritage from Pierre Trudeau to Brian Mulroney was the Access to Information Act. Nobody likes that.

One of the problems is that the bureaucracy thinks of the privacy and freedom of information acts together. They think they have to fix both at the same time. There's nothing that wrong with the Access to Information Act—I couldn't be here and be highly critical of it—but the Privacy Act is something different. We have to keep them on the Privacy Act focus because of the resistance on the freedom of information side. People don't like open, accountable government.

I happen to have been an information commissioner. I regard my work as an information commissioner as much more important than my work as privacy commissioner, but it doesn't mean the privacy commissioner work was trivial. I did a lot to help open up society in British Columbia so that people could know what was going on. I even opened *The Province* in Vancouver one day to see all my expense accounts flashed across the front column. It wasn't a charming experience, but it's what happens in an open and democratic society.

● (1635)

Mr. Sukh Dhaliwal: Technology changes every day. Do you believe there should be a statutory review of the provisions of the Privacy Act, and if so, how long should it be?

Prof. David Flaherty: Well, Quebec does it, I'm told, by the commissioner and by her submission, every five years. I think we do something like that in British Columbia and Alberta. It's a good thing to have people come before members of Parliament and say what they think. We were having members of the public, trade associations, automobile dealers, whatever it was, coming to say what they liked and disliked.

I have a rather jaundiced view because I worked three hard years on things that should be done to fix the Privacy Act and the Access to Information Act and nothing happened. There were some policy changes but no statutory changes. I think it was partly because Mr. Mulroney did not like the Access to Information Act, but I'm speculating.

The Chair: I'm sorry, but the clock does go quickly.

Mr. Van Kesteren.

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

Thanks for coming.

I'm listening to this debate back and forth, and I'm agreeing and I'm disagreeing. Quite frankly, I see your point, sure, but on the other hand, I'm thinking, who cares? Like, who really cares?

Prof. David Flaherty: Oh, this is going to be fun.

Mr. Dave Van Kesteren: Don't get mad at me, because I know you really get passionate about this.

But like, who cares if somebody knows I'm a Protestant or a Catholic? Why can't we say to government, “You can collect what you want, but don't let it out”, and keep it as simple as that?

I guess I'm like Mr. Tilson: I see, on the one hand, this bureaucracy just looming, and I shudder when I think about the implications.

Prof. David Flaherty: How much money do you have in your current account?

Mr. Dave Van Kesteren: Do you really want to—

Prof. David Flaherty: Have you ever had psychiatric care?

Mr. Dave Van Kesteren: No.

Prof. David Flaherty: What medications are you on?

Mr. Dave Van Kesteren: None.

Prof. David Flaherty: Do you care?

Mr. Dave Van Kesteren: Do I care?

Okay, the money part—I don't like that.

Prof. David Flaherty: Oh, you don't, eh? Isn't that interesting—well, well, well.

Mr. Dave Van Kesteren: I understand that. But nobody's ever disclosed that. If they would, I think I....

So they're collecting this stuff. I think some of us have a phobia about it. There's Homeland Security, yes, and so on. But it's kind of like climbing a hill because it's there: we have this technology so that we can collect all this stuff.

Let me just finish this last thought. Can you give me cited examples of where it has just wreaked havoc having this information? Because if we're going to change all these laws—I'm not saying we shouldn't, I'm just playing the devil's advocate here—then why? Why are we doing it? Why can't we just say to government, "You can collect this stuff, but don't you dare let it go"?

Prof. David Flaherty: In many ways, that's what we would like to do.

Do you believe you have a right to privacy as an individual?

Mr. Dave Van Kesteren: Sure.

Prof. David Flaherty: Is it protected under the Canadian Charter of Rights and Freedoms?

Mr. Dave Van Kesteren: Yes, it is.

Prof. David Flaherty: Is it a fundamental human right of Canadians?

Mr. Dave Van Kesteren: Yes.

Prof. David Flaherty: So you have three things right there. No one can function without privacy. There's never been a society on the face of the earth that didn't use privacy for certain practices, such as sexual relations.

I had a great story from a very open mother Tuesday morning in Vancouver, who told me that her daughter—16 and brilliant—asked her, "How often do you and Dad have sex?" She looked at the kid and said, "That's private."

At least I didn't get into your sex life.

Mr. Dave Van Kesteren: But I won't see on the front page of *The Globe and Mail* that somebody found out that I had, you know, psychiatric treatment, and that they've let this all go.

Prof. David Flaherty: But that's why we have laws in place.

Mr. Dave Van Kesteren: Exactly. We have these laws. If we're going to toughen them up....

I want to go one step further. We talked about past governments. I think I know the answer to this, although you might not like the answer. I listened to what you were saying in terms of Rock and Manley. Did they change any of the privacy laws?

Prof. David Flaherty: Absolutely.

Mr. Dave Van Kesteren: But I thought this thing was archaic and hadn't been changed in 25 years.

Prof. David Flaherty: No, you see, what they were doing was privacy law for the private sector. We have very strong privacy laws for the whole private sector that, in Alberta and British Columbia.... One of the people sitting beside me was the assistant commissioner for the private sector in Alberta. She and her colleagues did a terrific job of making the law meaningful for residents in Alberta in terms of the private sector. Why? Because they had a hell of a good law. And that's what we don't have here at the federal level. We have a really rotten law.

● (1640)

Mr. Dave Van Kesteren: I know, but we have....

I'm going to talk to you about the average joe. I mean, your buddy wanted to throw a glass at you because...why? I forget.

Prof. David Flaherty: I meant change.

Mr. Dave Van Kesteren: The point is that the average guy in the street wants to throw a glass at you because he's sick and tired of getting beat up on the street, or he wants to change the age of protection, or he's sick and tired of juveniles not.... That's reality to Canadians.

Justice departments are facing those types of challenges, so when they look at this they say, "All right, what are we getting so worked up about?" I'm asking you.

Prof. David Flaherty: I want the police, my friends in the police and in the RCMP, to follow the ten privacy commandments. I want them to catch all these bad people. I want them to end child pornography. I want them to use surveillance for that particular purpose. But privacy is a manageable issue.

So many of the issues you face in government or in opposition are hopeless. I'm watching people smoke out here on the streets, or people with obesity, or something like that. How are you going to make people eat the right food, exercise well?

Mr. Dave Van Kesteren: You want to do that, we'll talk about privacy.

Prof. David Flaherty: Privacy is easier to manage when there's a set of rules that you can put in place. It's a specialist issue. You don't have to become privacy experts. Know that there are ten privacy commandments. Remember that there are ten commandments in Christianity, in religion, if that's what your bag is, and you're supposed to be following them.

Remember, consent is crucial. Consent cures all. Most of the time you're engaged in consensual activity. I'm telling you things about myself because I choose to make a point, but other stories I'm telling you are anonymous.

Mr. Dave Van Kesteren: So to wrap up my statement, can we do this thing and just say "We're going to slap you really hard if you collect this stuff and..."? I don't mind doing these other things, but without building a huge bureaucracy.

Prof. David Flaherty: I would want to reorient the existing resources from other activities to making privacy management work, because it's in the best interests of every government institution. I'm anti-bureaucratic in several ways, as I've indicated, based on direct experience. I'm a one-person consulting shop. You might think no one would work with me, but that's not the case.

The Chair: Thank you very much.

I will have to excuse myself shortly—I have to catch a flight for an important meeting in Toronto—but there was a question I wanted to make sure we got the answer to. Perhaps it can be dealt with.

It has to do with the concerns around outsourcing. B.C. had some issues there. There was a need for blocking provisions—I assume that these are the criteria—to establish the applicability or the appropriateness of outsourcing. Did B.C. have to amend their legislation for that, and are the criteria effective and working now?

Prof. David Flaherty: I appreciate your asking me that question. As usual, I have all kinds of conflicts. I advised Sun Microsystems and MAXIMUS in their outsourcing wins in British Columbia. I think I advised EDS as well, but this is the MAXIMUS story. I'm a director of MAXIMUS for my sins, so you can take what I'm saying with a grain of salt.

The British Columbia government wanted to outsource the management of the Medical Services Plan, which is like OHIP in Ontario, and also PharmaNet, which has everybody's prescription history in it. There was a great reaction from the unions, so they went to court to try to block the outsourcing deal on privacy grounds. The response of the British Columbia government was to amend our Freedom of Information and Protection of Privacy Act to say all data processing has to be in Canada. The American company could have no direct links with the United States and could not have our personal information going back and forth to the United States. There had to be privacy training, privacy audits, etc.

The part of the story that I like is that we ended up with MAXIMUS B.C. Health, a subsidiary that runs these operations with the tightest privacy rules and security rules in the country. They have 400 staff that are being monitored all the time. They have to report privacy breaches within an hour of their happening. They have a chief privacy officer. They have online privacy training, and they have annual audits of their compliance by Deloitte Touche and people like that.

What's my problem with that? I have none whatsoever. That shows what good privacy protection could be put in place for reasonably sensitive personal information in British Columbia. But does the Ministry of Health do that? Do the Vancouver Island health authorities do that? Does Vancouver Coastal Health do that? No, they don't. They don't have the resources to do it, and nobody's making them do it. They might have privacy officers, but they don't have the resources to do the job.

Vancouver Island, where I live, has 45 different places like hospitals and things like that. There's one half-time person doing privacy protection for the Vancouver Island Health Authority. There is a population of probably 750,000 people. MAXIMUS B.C. Health is providing an excellent service. The Minister of Health has said that. The deputy minister of health has said that. People are happy working there. The same workforce came from the government and was privatized. It's working very well, and it's making money. It's not making a hell of a lot of money, because they signed a pretty tough contract, and the government really watches them. Why isn't the government watching itself according to the same standards? That's my point, especially with regard to the e-health field.

● (1645)

The Chair: Thank you kindly.

Mr. Hiebert, please.

Mr. Russ Hiebert (South Surrey—White Rock—Cloverdale, CPC): Thank you, Mr. Chair.

Mr. Flaherty, I intuitively support your propositions, since I'm an opponent of big government. I'm an opponent of big brother snooping into the privacy of my life or anybody else's life mostly because I'm concerned about the potential abuse of power. Information can provide power to individuals who want to manipulate or extort or, in the case of identity theft, impersonate individuals.

I recognize those concerns. A couple of minutes ago you responded to the question of one of my colleagues about why we should be concerned about this. You asked whether he was taking drugs, whether he had ever had psychiatric care, what the balance of his bank account was. The drugs and psychiatric care are provincial responsibilities, and the bank account information is a private matter that PIPEDA would apply to.

So I want to hear from you, from a federal government perspective, apart from identity theft, apart from people stealing people's social insurance numbers and birth dates and impersonating them, what other example of a risk you can think of that the federal government is trying to prevent.

Prof. David Flaherty: I was using those specific questions to establish if he had any sense of privacy, which we quickly established he does, as most of us do.

Regarding the federal government, I describe agencies and departments as privacy-intensive if they collect a great deal of personal information. So Human Resources Development Canada, Revenue Canada, Health Canada, Canada Border Services Agency, the RCMP, Canada Post to a lesser extent—these are examples that come to mind of places where there's a heck of a lot of personal information—

Mr. Russ Hiebert: And each one of these departments you've mentioned has very strict legislation and codes or regulations that prevent them from sharing that information, especially Revenue Canada.

Prof. David Flaherty: With all due respect, I'm not sure that's indeed the case, and I say that from the basis of my consulting work. In my paper, which I'll be sharing with the committee shortly, once it's translated, I use Health Canada, as I explained earlier, as a pretty good model, and I think I had something to do with stimulating them to put privacy risk management strategies in place.

I don't really know enough. Certainly one of the recommendations of the Privacy Commissioner in her audit of the Canada Border Services Agency two or three years ago was that they should do the same sort of thing, because they're into the same privacy risk management strategy as I am, but it's still a work in progress.

So I appreciate that you think the glass is half full when I think the glass if half empty, and there's obviously a bit of a difference of opinion, but I don't have a comfort zone, nor have I done the empirical work to really give you as many illustrations as you might like, to be comforted that in fact the rules and regulations in the Privacy Act are being complied with the way they should be to meet the challenges of the 21st century.

Mr. Russ Hiebert: Just to correct your impression, I'd like to believe that it was my persistent cajoling of this committee that brought this Privacy Act review to its attention. I've been doing so for about six months, so you have me to blame for being here today. But I'd still like to get a sense—

[*Translation*]

Mrs. Carole Lavallée: A point of order, Mr. Chair. *[Editorial note: inaudible.]*

[*English*]

Mr. Russ Hiebert: That's not a point of order.

I'd still like to get a sense from you, if you could provide an example of a specific risk we are facing. What's something tangible we can take to Canadians to say this is why we need to get this done, this is why we need to adopt these recommendations?

Prof. David Flaherty: I'm going to use a provincial example, because the report came out yesterday. New Brunswick was shipping personal information on 750 people from B.C. who had been treated, I guess, in New Brunswick. British Columbia was going to pay the Ministry of Health. The Ministry of Health was shipping data on tapes from New Brunswick's Ministry of Health to British Columbia, to Victoria. Guess what they did? They sent them by courier unencrypted on disk. Guess what? They were lost. So now the commissioners from New Brunswick and British Columbia issued a report yesterday about how lousy the security was. They should have been using much more modern ways of doing it. It should have been sent electronically to start with.

That's a very specific example that was all over the newspapers in both New Brunswick and British Columbia, and it led the Ministers of Health to be very embarrassed politically, to be beat up on by the opposition in their Houses, to have to make embarrassing admissions that they'd lost the damned data. Does that move you?

● (1650)

Mr. Russ Hiebert: A federal example, then, to extrapolate, would be that if the federal government were transferring data about Canadians—tax information, potentially, or RCMP files—to another department within the government, and that data was lost, then, potentially, somebody could use that data and embarrass and extort. Is that the concern?

Prof. David Flaherty: The problem I have is that a lot of the privacy breaches I'm aware of I have knowledge of under confidentiality agreements with my clients. I can't come and whistle-blow on my clients, but let me assure you, there are far more breaches taking place, which are far more sensitive in nature than you even read about in the newspaper. Hardly a week goes by that there isn't another privacy disaster that has happened.

Mr. David Tilson: Thank you.

Mr. Dhaliwal.

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

I'm going to continue where you left off, Mr. Flaherty.

You have a lot more examples that you don't want to disclose, and we don't want to hear them. But certainly, from a general perspective, as Mr. Hiebert was saying, most of the security breaches or these privacy breaches are provincial matters.

From your experience, even though you don't want to disclose them, are there many breaches that occur at the federal level, in general?

Prof. David Flaherty: There are some reasons, which I'm not going to go into in public, why I've been doing less federal work the last couple of years than I did from 1991 to 2003 or 2004. The best examples I can use are from the provinces and territories. You should be aware that Manitoba announced last week that it was finally going to set up a proper privacy commissioner and, to the best of my understanding, take the power away from the ombudsman, who had too many other things to do, and give the Privacy Commissioner of Manitoba regulatory power. I think that's considerable progress. There's an excellent privacy commissioner in Saskatchewan, who doesn't have regulatory order-making power, and he would love to have it, because he can't do much when records are found in boxes on the street, or patients' records are found all over the place.

What we don't hear about, because they are very technical breaches, is the number of times data that has identifiers on it is disclosed—personal health numbers, for example, and things that should not have been disclosed—because of sloppiness or human error. So going back to the point you were making earlier, I want as many privacy-enhancing technologies as possible.

As I may have already said to you, I want machines watching machines. I want that, as do the banks. The banks are just bringing this in now. If a teller in Prince George is always communicating with Rimouski, something's wrong, because most of our customers should be up there. If a nurse in the genetics department is always looking up people in emergency, there's something odd there. Using an electronic system, we can monitor that, and a security person or a privacy person working for the organization could check it out. It could be like a TILDE system.

So this is the way we can use technology that already exists to audit and to monitor transactions. The Social Security Administration in the U.S. and American Express have done that kind of thing for a long time. My understanding is that the Canadian banks are just bringing in more of that kind of monitoring.

Mr. Sukh Dhaliwal: On the other hand, we also hear from some of the members of the committee that the Privacy Commissioner has a backlog, that she's trying to deal with that situation. But when she was here and I asked her the question, she didn't ask for any more resources than she's had for the last years. She said she could handle that situation.

How much extra pressure would it put on the Privacy Commissioner and her department if the reforms that you have in mind were enacted by the justice minister?

Prof. David Flaherty: I'm a typical academic in the sense that I'm not very good at answering resourcing questions.

It would not be a trivial cost but I don't think it would be major. I think everybody working for a government or a private sector has to work more efficiently, has to work smarter, has to focus on what ought to be done. They should be using more individuals to do things rather than groups of people doing things.

The privacy experts in the Privacy Commissioner's office should be meeting with the privacy experts in these various ministries and sorting out issues in a conciliatory fashion, not fighting like this. I call them privacy watchdogs, but I want them to be non-confrontational, to win the attention of the people who are supposed to be regulating, to depend on goodwill, to promote privacy interests properly, to recognize that eventually Parliament is going to decide anyway. If Parliament doesn't decide properly, the courts can tell Parliament they didn't do it properly, just as they could tell the Privacy Commissioner they didn't do something properly.

● (1655)

Mr. Sukh Dhaliwal: On the one hand, I agree with you that we have to protect the privacy of Canadians. But that's to do with their dignity, with their personal perspective. Are there any economic benefits that would come with these increased privacy laws?

Prof. David Flaherty: Richard Posner, the famous U.S. judge and economics professor, has a book on the economics of privacy. We argue, rhetorically, that privacy is good for business, that privacy is good business, that when you go to Costco or anyplace else and they tell you up front what they're going to do with your personal information and then they do it.... They have a massive database at Costco of 50 million employees on a North American basis. Obviously they're treating them properly and are not doing untoward things with them—profiling or extra things that would be untoward or that they didn't say up front.

You see, if you're open and transparent about what personal information you're going to collect, use, disclose, retain, and store, then people will know, if you go to whatever kind of person you're dealing with or with the federal government, what's going to happen.

Mr. David Tilson: Thank you.

Mr. Hiebert.

Mr. Russ Hiebert: Thank you, Mr. Chair.

I'm going to try to pick up where I left off and give you another opportunity to explain the real reasons behind why we need to make these changes. I've asked you for specific examples. You've suggested that for confidentiality reasons you can't discuss how this applies in the private sector. You've given us some provincial examples.

The only federal example that I can think of immediately would be Canadians' tax records. That is because of the possible embarrassment or the negotiating position that might emerge if all this information were made public. I also understand that there are severe consequences for this information being leaked from Revenue Canada, including Criminal Code sanctions. So I think there's a very strong disincentive for that to happen.

Can you think of another commonplace example of where we could use this as a justification for this massive change we're talking about, this massive expense that might emerge if we pursue this path? In other words, what are the consequences of not addressing these concerns?

Prof. David Flaherty: I don't like making public policy by anecdotes, but the Institute for the Study of Privacy Issues, which I subscribe to, every day sends me 30 to 50 English-language newspaper clippings from around the world and all over Canada about privacy breaches of the day.

What I'd like to do is get your e-mail address and send you one a day for a while. You can build up your archive of these sorts of things.

Mr. Russ Hiebert: Sure.

Prof. David Flaherty: The biggest privacy disaster in the public sector in English-speaking countries in the last several months was in November or December. Tapes were lost in the United Kingdom, moving by courier from one government department to another, with information on something like 25 million people. It was some huge mass of data. It brought the government of Gordon Brown to a halt and increased the powers of the information commissioner and so forth. It was just a huge scandal. It was in our newspapers every day for a relatively long period of time.

I don't want to see that kind of thing going on. I want the average Canadian to be satisfied that if they give their personal information to the Canadian government, the Privacy Commissioner is there as a privacy watchdog, that rules are in place that are sophisticated and ready for the 21st century, and that the rules are going to be followed.

I am a pretty good fan of how the private sector is complying with PIPEDA and with the legislation in British Columbia and Alberta, but every month or two Alberta is whacking somebody—Winners or somebody like that—for doing things they shouldn't be doing. So there's still a big learning curve.

Mr. Russ Hiebert: The case of private sector privacy is very clear. Profiling and other economic incentives give people the motivation to take that data, distort it, change it, and use it in ways Canadians don't address. I'm more concerned about the federal government.

Prof. David Flaherty: That's great, by the way.

Mr. Russ Hiebert: You suggested earlier in this meeting that if we were to adopt these ten recommendations all at once it would bring the government to a halt because of the impact it would have. Without chief privacy officers in each of these 250 departments, where would you start?

Do you have any recommendations on how this would roll out? Would you suggest a delayed ten-year timeframe to apply this information requirement, or can we all do it on day one?

Prof. David Flaherty: I can't believe it. It's as if you're living in a 25-year-old house that hasn't been redecorated, and I'm the designer coming in to help you. And you say where should I start? Should I do the furnace first? Should I put a new roof on it? Do I do this, that, and the other thing. I'm not trying to be too facetious. I'm certainly not suggesting these ten recommendations of the Privacy Commissioner of Canada would bring the government to a halt, but in some ways they're so weak and namby-pamby. I mean, she's being a good person giving you easy things to do, so do them. But there's a heck of a lot more things. I think I had 40 or 50 points, and even more, in my paper. This is a whole housecleaning. This house is rotten. I'm exaggerating, and it's not going to bring the government to its feet. There are rules and regulations.

It would be as if a minister were preaching to the converted with one-third of the Bible at his disposal. Let's have the whole shooting match to work with.

● (1700)

Mr. Russ Hiebert: Okay.

You talked about having specific privacy officers for each government department. Fair enough. Is there a case to be made that it would perhaps be more cost-effective to train existing management within those departments, to add this responsibility to them?

Prof. David Flaherty: I think Health Canada's privacy champion is at the ADM level. The only reason they didn't make him or her the chief privacy officer was because there was no tradition of doing it.

I think the Canada Millennium Scholarship Foundation here and the federal government have a chief privacy officer. Some others are scattered around. The Government of Ontario, as I point out in my paper, has a chief privacy officer. Every senior manager has to have some understanding of what privacy is all about. You can see I started by trying to tell you these ten simple principles are all you need to know, but once you get into it it's complicated. The privacy impact assessment gets into the niceties of security of encryption standards and of data-sharing agreements.

Mr. David Tilson: Thank you.

Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: Thank you very much.

First, Professor Flaherty, let me say that I do not quite agree with what you said about the Access to Information Act. Personally, I think the act is as quaint, as you said, as the one we are talking about today. I think, for example, about section 15(1), which is never justified, and about the timelines that are never, or very rarely, followed. It is a real disaster. Furthermore, it is impossible to file lawsuits and you can sometimes see departmental interference. All these reasons, and any number of others, lead me to think that dealing with access to information is extremely urgent. Personally, I would have liked to study the Access to Information Act before the Privacy Act. Unfortunately, Charles Hubbard voted on behalf of the Liberals and Russ Hiebert, I am afraid, will have to concede that he is not the father of the study we are currently doing.

Earlier, we looked at the ten recommendations and you said that you were all in agreement on them. The intent of recommendation 6 is for the commissioner to have greater discretion to refuse or discontinue complaints. You said that you agreed completely with that recommendation. I think that giving the commissioner discretionary power would pose no problem at the moment, but still, we cannot see into the future. Would it not be better to specify the kind of complaint that she must refuse or discontinue? Would it not be better to do that than to say that she can discontinue a complaint at her discretion?

[*English*]

Prof. David Flaherty: I was shocked to learn the other day that there are now 13 federal officials—the ombudsman, Auditor General, and stuff like that. The reason I was shocked was this: imagine the risks, the increasing risks, of putting weak people or ineffective people in those jobs. That's the kind of concern I have about these high-level positions.

I've known every privacy commissioner of Canada—with the exception of Mr. Radwanski, and I'm not commenting on him—and they were all wise people. They were sound individuals. What we're talking about is how do you focus the limited resources of the office? Investigating one complaint after another is not effective if there are better ways to spend your time, doing auditing, site visits, education, policy advice, and so forth.

I must say, if you invited me back, I could give you a lecture on reforming the Access to Information Act or any other freedom of information act. My focus would be similar to what it is on Privacy Act compliance. You have to have a good law in the Privacy Act, but I'm interested in how you get effective compliance. What are the mechanisms you have in place? How do you educate people to accept a freedom of information act?

In British Columbia, when I was first visiting a certain deputy minister, he said, “Look, we have an ombudsman, we have an auditor general, we don't need an information and privacy commissioner.” I persuaded him, over the course of a year or two, to the point where he became a champion in cabinet and with his fellow deputy ministers on the importance of openness in society. That's the kind of thing I would be arguing on the Access to Information Act, which is not what you're dealing with here.

I'm delighted that this committee exists and has this broad focus. I think it's damned important. You have your work cut out for you over time.

[*Translation*]

Mrs. Carole Lavallée: There are other recommendations that, to my knowledge, are found neither in your document nor the commissioner's. For example, on several occasions, you mentioned the loss of data when it is being transported. Why do we not include a way to transport data in the legislation?

I would also like to talk about the way of destroying data. I say that so that we can organize our time accordingly.

● (1705)

Prof. David Flaherty: You understand that, in the 1982 act,

[*English*]

there is no security standard at all. What we put in the other pieces of legislation in the public sector across Canada is a reasonableness standard: as PIPEDA asks, what would a reasonable person expect to have happen?

Well, no wonder security breaches are happening and then the requirements for breach notification, which should be in the law as well. People don't take it seriously enough, and they're sloppy. It's very difficult to do good security because it's routine work. As much as possible, we have to have machines doing it, and we build in the kinds of sophisticated security regimes that we have here.

I actually think that the federal government, being the federal government, probably has quite sophisticated security practices, and the RCMP has threat risk assessments and all this stuff. That's an integral part of privacy protection. That part is probably not as big and bad as some of the other areas, the lack of consent and things like that.

[*Translation*]

Mrs. Carole Lavallée: Do you not think that we should include mechanisms for transporting data in the act? No one has recommended it until now.

[*English*]

Prof. David Flaherty: That's why I mentioned earlier, Madame Lavallée, the idea of data-sharing agreements. They will say not only what personal information is being exchanged between Quebec, Ontario, and the federal government, but how it's happening and what the transfer mechanism is. That would really be part of reasonable security. It's in the security domain.

I think where you're leading, or where you should be leading, is to breach notification. We really should be informing Canadians when the data goes missing, not a month later. Our friend on the government side was talking about identity theft. It's a very serious matter. My credit card was compromised in the last month. I was very unhappy. It had never happened to me before. I didn't feel like my house had been burglarized, but it was a very unpleasant experience.

Mr. David Tilson: Yes indeed.

Mr. Dhaliwal.

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

Mr. Flaherty, I met with a couple of individuals yesterday. It had to do with another topic, but I'm going to come back to this issue from there. The topic had to do with no-call numbers, where people can't call you unless it's for particular purposes. One of the purposes is for market research, which is very important in terms of dealing with the situations of new research, innovation, and technology.

Where would you draw a line between collecting personal information from a privacy perspective and information that can be used for research purposes?

Prof. David Flaherty: It might surprise you, given some of the positions I've taken, that I'm a great fan of research and public health surveillance, and big research projects. I have some wonderful clients at UBC who are doing wonderful work in child care, child protection, and things like that, the monitoring of children's health and vision and hearing over time. I simply make sure their privacy house is in order, which is the important component, so there will be no privacy problems that emerge when the work goes forward.

I dislike intensely being telephoned at home by people I don't want to hear from, so I can't wait to get on the do-not-call list. Michael Geist from the University of Ottawa set up his own do-not-call list, and I jumped on it the first day. I do recognize the importance of market research, of political polling, of Ipsos Reid finding out what Canadians think about this, that, and the other thing. There is a bit of a fine line. Some people love getting phone calls. Some people love getting junk mail, and that's an individual right. I used to complain more about junk mail than I do now, because between my mailbox and my office there's a garbage can, and I dump what I don't want to look at into the garbage can.

That's not much of an answer, and I really don't have anything very intelligent to say about the do-not-call business. As in everything else, there's a balance. We have to have a balance between our privacy interests and law enforcement, between our privacy interests and national security, between the need to give information to get health care and confidence that it's going to be properly protected when we give it out.

Actually, I should have given you some health care examples. That would have been easier, because that's what I work in most of the time.

Mr. Sukh Dhaliwal: Thank you for coming out.

Mr. David Tilson: Mr. Geist is coming, apparently, so we'll ask him those questions.

Mr. Hiebert, and then Monsieur Nadeau.

Mr. Russ Hiebert: Identity theft is an issue Canadians have expressed a concern about. With respect to the government and with respect to individuals, how can the government help prevent identity theft? How can individuals protect themselves?

● (1710)

Prof. David Flaherty: I have a whole shtick about how important it is for people to be sensitive to privacy as a human right, to be concerned. One of the good things these privacy commissioners have done is to give parents kits for their kids and training for schools about being careful with Facebook, and about giving out information on the phone and things like that as part of general education.

I actually believe that at the end of the day, everybody has to be their own privacy commissioner. I'll leave that idea with you. You shouldn't simply depend on the Privacy Commissioner of Canada to protect your privacy interests, but if there's a problem, you should be going to the Privacy Commissioner to make a complaint. Then you should expect her, in the highly sophisticated areas such as what Statistics Canada or Revenue Canada are actually doing with our personal information.... Despite saying they're going to do X, are they doing Y? Who's checking on that? Who's the inspector?

Mr. Russ Hiebert: I haven't heard an answer to the question about what Canadians can do. I appreciate the personal encouragement to be a privacy protector for yourself, but on the topic of Stats Canada—this came up at the last committee meeting we had—do you think Stats Canada should have the right to require Canadians to provide personal information?

Prof. David Flaherty: Well, Parliament, around 1905, when they first enacted the Census Act, said yes, it does.

Mr. Russ Hiebert: What do you think?

Prof. David Flaherty: One of my first privacy books, published in 1978 or 1979, was about statistical agencies around the world. The theme of it was the importance of using individual data for epidemiological research and statistical research and so forth. The strongest privacy legislation in the country governs Statistics Canada. They cannot give out identifiable information under any circumstances. As each piece of legislation goes through Parliament, whatever it is, if it involves personal information, you should be putting in privacy provisions, specialized ones that apply to a law enforcement database like CPIC or a Health Canada public surveillance database, or whatever it is.

A really neat way of strengthening the Privacy Act is to stick the privacy stuff in it as each bill goes through. It's a more specialized form of data protection, something they do very well in the United States, by the way.

Mr. Russ Hiebert: So you don't have any problem with Stats Canada collecting all kinds of personal information?

Prof. David Flaherty: I'm a professor and I'm a researcher. I just did the work for the regional health survey for the Assembly of First Nations. I asked if they really wanted to be going into homes and asking children, adolescents, and adults these kinds of extremely sensitive, personal questions about drug use, sexual abuse, residential schools, and sexual practices. They said they'd only go in there with the consent of the chief and council, and if it was consensual. In my privacy impact statement, that was one of the questions asked. They said, “We need to know this information”.

Mr. Russ Hiebert: Should Canadians have to give their consent to Stats Canada to fill out their forms?

Prof. David Flaherty: The census of population is certainly mandatory. I loved it when I was Privacy Commissioner. I had an employment survey, and they were all nervous about what was going to happen, but I was quite happy to participate. I watched them like a hawk. They didn't do anything wrong. Again, in the footnotes to my essay, I've cited Ivan Fellegi, the Chief Statistician of Canada since kingdom come, as an excellent example of a model person who's put privacy mechanisms in place at Statistics Canada to manage privacy quite well. I used to get a lot more work from them, and I'm not getting it now because they've put their own house in order.

Mr. David Tilson: Okay.

Mr. Nadeau.

[*Translation*]

Mr. Richard Nadeau: Thank you, Mr. Chair.

Earlier, you mentioned risk management. Could you be more specific and tell us, in concrete terms, how we can make sure that we manage risk adequately and in accordance with the legislation?

[*English*]

Prof. David Flaherty: I was working with a client in British Columbia last year, a crown corporation with a lot of sensitive personal information. It did an assessment of the risks involved in its public sector and private sector relationships. It was a very sophisticated management review of what the privacy risks were, and it even involved a rating scheme of one to ten. I was really skeptical about this, but it was quite well managed, and they ended up with the top ten privacy risks to this crown corporation. They were able to do it based on a whole bunch of people inside the organization pulling together.

I don't think that's being done in the federal government, but I don't really know. It should be. And the reason I talk about privacy risk management is that senior executives are having to deal with risk management all the time. I want the financial risk management, labour relations risk management, and even resources risk management to put on their risk management hats when they think about privacy. And there the risks are that data goes missing, that data is used for unintended purposes that it's not supposed to be used for, that it's used to harm individuals, or it's stolen, or it's used to invade their privacy by people who are browsing databases, or it's sold to criminal elements.

● (1715)

[*Translation*]

Mr. Richard Nadeau: I have another question, Mr. Chair, dealing with destroying documents.

We know the process. There comes a time when a document is considered to be no longer useful. How do you see the process of destroying documents?

[*English*]

Prof. David Flaherty: There's probably nothing more important that could be done to protect the privacy of Canadians than to destroy more personal information. I mentioned to you earlier that I've worked for organizations that have been in existence for 25 or 30 years or even longer. They've never destroyed anything, partly sometimes because they don't have a records management schedule. They have 85,000 boxes in storage at the expense of the taxpayers. It's just crazy.

Hospitals do quite a good job. If you haven't been there for nine years, they destroy your health record. If you were born there and you keep going back every year, you'll have a cradle-to-grave health record. That's perfectly acceptable.

So you want an economic argument. Let's get rid of these huge warehouses of records that are of no possible use. No one could ever use them again. If they're of historical significance, the archivists know how to clean out the stuff that's of historical significance, like your memoirs or your letters, whatever it is. So data destruction is incredibly important.

The French in France have a wonderful concept in their privacy law called *droit à l'oubli* , the right to be forgotten. It's a very important concept. We need to import that into Canadian privacy practice, not so much into law. Get rid of records. If you don't need them, burn them.

Mr. David Tilson: Monsieur Nadeau, are you finished?

[*Translation*]

Mr. Richard Nadeau: I have one more question, Mr. Chair, and it will be my last one.

I am looking for simple examples. We have been talking about our fellow citizens, about bills we are working on, particularly this one, dealing with personal information. It affects us all. We ask ourselves how private is our private life really if government, corporations and companies can come and dig around in our private lives. You gave examples earlier. Do you have simple examples that make a solid argument for the relevance of amending this legislation to protect Canadians in an appropriate way?

[*English*]

Prof. David Flaherty: I explained earlier when I was asked a similar question that some days I remember wonderful horror stories. Some days I remember them less. This happens to be a day when horror stories are not springing to mind, partly because I like to put them out of my mind, because they're often so appalling they shouldn't have happened. I think if you just pay attention to your daily newspapers for the next month or so, you'll come up with lots of privacy horror stories—that's how we refer to them—or privacy disasters, things that shouldn't have happened.

What is so important is that 30% or 40% of the population, it is estimated, is very sensitive about their personal privacy. You ask them for their social insurance number, and they get really excited, even though I know if you have a social insurance number you can call up Bathurst, New Brunswick, where the social insurance number registry is, until you're blue in the face, and they're not going to tell you anything.

So one of the reasons to get sound privacy management in place for the federal government, based on strong legislation, is to have reduced paranoia in the population, to be able to feel that in fact the Government of Canada is respecting your personal information, taking it for legitimate purposes, using it in authorized ways, destroying it when it should be destroyed, linking it when it's supposed to link it to profile you for disease risk, for example.

I'm incredibly enthusiastic about what I gather are some forthcoming initiatives to monitor larger groups of the population for health over longer periods of time. That can be done in a very privacy-sensitive way, and it's very much in the public interest, so it's not as though I'm sitting here as a Luddite.

Mr. David Tilson: Thank you.

Mr. Hiebert, and then Mr. Norlock.

Mr. Russ Hiebert: Mr. Flaherty, earlier you talked about these ten commandments that apply to the private sector. One of them was consent. You referred to it as the law of "adultery".

In my last set of questions, we talked about Stats Canada. You seemed to suggest that Canadians should not necessarily be required to give their consent because Stats Canada does such a really good job of protecting their privacy.

Would it be fair to say that this requirement for consent has a different standard when it applies to the government from when it applies to the private sector? Because the government is a different institution—it's there to serve the community and doesn't have private economic interests—is there a different standard?

Prof. David Flaherty: Certainly Parliament has decided that there's a much higher consent standard for the private sector than for the public sector, because there's almost no consent standard. There is a requirement in the Privacy Act that you should only use personal information without the consent of the individual for very, very limited purposes.

I was trying to turn the tables on you, in a way, by asking who set the consent standard for Statistics Canada; it was Parliament, particularly for the census of population. My recollection is that most of the rest of their surveys are consensual. They don't come to you and say "You're in this survey for five years." So it's not a good example of the consent thing.

If you go to your doctor, he's operating on the basis of informed consent. If you go to the bank nowadays—and it should be the same with Revenue Canada—in the initial transaction you have with them you should know what their privacy practices are, that they don't disclose your identifiable personal information to anybody without your consent. And they're pretty good at that. I have an accountant who does work for my company. They make me get a signature, through my accountant, to Revenue Canada, that the accountant can discuss my personal affairs. They're very cautious.

● (1720)

Mr. Russ Hiebert: I guess the point I'm trying to make is that we can't just directly adopt the ten commandments of the private sector privacy principles into the public sector sphere. Issues like consent and perhaps other ones—I haven't probed them—don't simply apply in the same way.

Prof. David Flaherty: I don't agree with what you're saying, with all due respect. I want to push the....

And I'm being a bit of a privacy advocate here—a privacy radical, almost. Some of my friends behind me might not agree; they're free to speak their minds in due course.

I want as much consent as possible. Obviously, if I go to an emergency room and I'm unconscious, they can't get information. There the issue is consent to treatment versus information consent. You know we're talking about information consent, and you're perfectly right about that. I want my relationship with the federal government to be as privacy-sensitive as is my relationship with my investment brokers, with my auto plan agents in British Columbia, etc.

Mr. Russ Hiebert: Yes, but if the RCMP stops you, or if the CBSA officer holds you up at the border, or if the tax auditor comes to your business and says "I want your information", governments can't reasonably suggest that if you withhold your consent, you don't have to answer. So there's a different standard.

Prof. David Flaherty: Yes, yes, there are different obligations.

There was a wonderful cartoon last weekend in a national newspaper. In the cartoon somebody opens the door to "Audits"; the answer is, "I'm not interested".

Obviously there are obligations and duties of government that have to be carried out. Sometimes information is collected about us coercively. But the Supreme Court of Canada said recently, "Thank you very much, but you can only use sniffer dogs at Greyhound terminals and schools under certain circumstances, where there's reasonable cause." It may very well be that crossing the border, somebody will....

I was once stopped going to England because I smiled at somebody—last time I smiled at one of these characters. They harassed me. And I'm such an innocent abroad.

The argument I want to make to you is that if you've had such a high privacy standard for the private sector, which you have done in PIPEDA—and in Alberta and British Columbia with PIPA, and with the Quebec legislation—why do you think you'd let the government off the hook? It's not that we want the government to stop doing what a government should be doing, but they have to follow the rules of the road with respect to collection, use, disclosure, security, destruction, retention, records management.

Mr. Russ Hiebert: Thank you.

Mr. David Tilson: Mr. Norlock says he has one question.

Mr. Rick Norlock: Yes, well....

Prof. David Flaherty: When am I going to stop talking—that's probably the question.

Mr. Rick Norlock: No, no, not at all. I find you very informative.

Mr. David Tilson: One question.

Mr. Rick Norlock: I want to go back to how the Privacy Act would work under your recommendation, the most simplistic way, without growing that bureaucracy that we both do not want to grow.

It seems to me, having come from another government, that what you're saying is we have currently the Privacy Commissioner and her staff, and we really don't need to grow it much more, but what we do need to do is bring in these recommendations and reduce her workload so that she and her staff—through dictates, through the government, and the acceptance of other government departments—can train people already existent in those departments on how they can best ensure that the Privacy Act functions in their department. And if that occurs, if that's your recommendation, then really, other than the good legislation, not much more needs to be done.

Is that a correct way to summarize what we've been talking about?

Prof. David Flaherty: That's an excellent explanation of what I'm after.

What happens right now is that government departments say it's up to the Privacy Commissioner to make the Privacy Act work, even if it's lousy. And Treasury Board has not done its work except on the policy side.

In the 1980s Peter Gillis provided a lot of leadership on the administrative policy side to make the Privacy Act work in practice. But the government has to do more to implement the Privacy Act by getting people outside the Privacy Commissioner's office who know what they're doing—chief privacy officers—exactly as you described it. And then there will be less of a burden on the Privacy Commissioner's staff because they will build a sensitivity to privacy, a privacy culture, and privacy champions into the work of all federal institutions.

And everybody has personal information. We haven't talked about privacy rights of employees here. You have 217,000 people in the federal government whose personal information from an employment place is all over the place with all kinds of service providers, with all kinds of disability providers, and the contracts may or may not extend the privacy obligations of the employer, the Government of Canada, to the service providers. That's a whole kettle of fish.

One of the great things in British Columbia was a privacy protection schedule that, out of the U.S. Patriot Act brouhaha, mandated that universities, corporations, crown corporations, government institutions always put this privacy protection schedule into contracts with service providers who could be anything from Sun Microsystems or IBM to Manulife and a whole bunch of them. So there is an incredible amount of work to be done.

And the government institutions have to do much of it themselves as part of due diligence and prudent management of information if they're going to continue to have the confidence of Canadians.

● (1725)

Mr. David Tilson: Mr. Flaherty, thank you very much, sir. You've survived—

Prof. David Flaherty: Barely.

Mr. David Tilson: —almost two hours by yourself, and we do appreciate that you've given us a lot of food for thought. Thank you kindly on behalf of the committee.

Unless there is anything else, the meeting is adjourned until Tuesday, May 13, at 3:30.

Thank you, sir.

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

The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.

Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.