



Fourth Session, 38th Parliament

REPORT OF PROCEEDINGS
(HANSARD)

SPECIAL COMMITTEE TO REVIEW THE
**PERSONAL INFORMATION
PROTECTION ACT**

Vancouver
Friday, February 22, 2008
Issue No. 6

RON CANTELON, MLA, CHAIR

ISSN 1913-4746

**SPECIAL COMMITTEE TO REVIEW THE
PERSONAL INFORMATION PROTECTION ACT**

Vancouver
Friday, February 22, 2008

Chair: * Ron Cantelon (Nanaimo-Parksville L)

Deputy Chair: * Harry Lali (Yale-Lillooet NDP)

Members: * Mary Polak (Langley L)
* John Rustad (Prince George-Omineca L)
* Leonard Krog (Nanaimo NDP)

**denotes member present*

Clerk: Kate Ryan-Lloyd

Committee Staff: Josie Schofield (Committee Research Analyst)

Witnesses: Serge Corbeil (Insurance Bureau of Canada)
Darrell Evans (Executive Director, B.C. Freedom of Information and
Privacy Association; B.C. Civil Liberties Association)
Richard Gallagher (British Columbia Cancer Agency)
William Gibbens
George Greenwood (Canadian Identity Resources Inc.)
Anne Landry
Steven Lingard (Insurance Bureau of Canada)

CONTENTS

Special Committee to Review the
Personal Information Protection Act

Friday, February 22, 2008

	Page
Election of Chair and Deputy Chair	39
Presentations	39
G. Greenwood	
R. Gallagher	
D. Evans	
S. Corbeil	
S. Lingard	
A. Landry	
W. Gibbens	

MINUTES

SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT



Friday, February 22, 2008
9 a.m.

CN Strategy Room 2800
Segal Graduate School of Business, Vancouver

Present: Ron Cantelon, MLA (Chair); Harry Lali, MLA (Deputy Chair); Leonard Krog, MLA; Mary Polak, MLA; John Rustad, MLA

1. As there was not yet a Chair elected to serve the Committee, the Clerk Assistant and Committee Clerk called the meeting to order at 9:29 am.
2. **Resolved**, that Ron Cantelon, MLA be elected to serve as Chair of the Special Committee to Review the *Personal Information Protection Act*. (Leonard Krog, MLA)
3. **Resolved**, that Harry Lali, MLA be elected to serve as Deputy Chair of the Special Committee to Review the *Personal Information Protection Act*. (Leonard Krog, MLA)
4. Opening remarks by Ron Cantelon, MLA, Chair
5. The following witness appeared before the Committee and answered questions:
 - 1) Canadian Identity Resources Inc. George Greenwood
6. The Committee recessed at 9:44 am to 9:56 am
7. The following witnesses appeared before the Committee and answered questions:
 - 2) BC Cancer Agency and BC Cancer Research Centre Richard Gallagher
 - 3) BC Freedom of Information and Privacy Association;
BC Civil Liberties Association Darrell Evans
 - 4) Insurance Bureau of Canada Serge Corbeil
Steven Lingard
 - 5) Anne Landry
 - 6) William Gibbens
8. The Committee recessed at 11:33 am. to 11:50 am.
9. As no further witnesses were present, the Committee adjourned to the call of the Chair at 11:51 am.

Ron Cantelon, MLA
Chair

Kate Ryan-Lloyd
Clerk Assistant and
Committee Clerk

FRIDAY, FEBRUARY 22, 2008

The committee met at 9:29 a.m.

Election of Chair and Deputy Chair

K. Ryan-Lloyd (Clerk Assistant and Committee Clerk):

Good morning, everyone. My name is Kate Ryan-Lloyd, and I serve as the Clerk to the Special Committee to Review the Personal Information Protection Act. As this is the committee's first meeting in the new, fourth session of the 38th parliament, the first item of business will be the election of a Chair this morning. I'd like to open the floor to nominations to that position.

L. Krog: I would nominate Ron Cantelon, the MLA for Nanaimo-Parksville.

K. Ryan-Lloyd (Committee Clerk): Are there any further nominations?

Seeing none, Mr. Cantelon, would you accept the nomination?

R. Cantelon: I would.

K. Ryan-Lloyd (Committee Clerk): Okay, I will put the question.

Motion approved.

[R. Cantelon in the chair.]

R. Cantelon (Chair): Thank you, colleagues.

The second order of business is to nominate a vice-Chair for the committee.

[0930]

L. Krog: I would nominate the member for Yale-Lillooet, Harry Lali, who I understand has consented to serve in the position.

R. Cantelon (Chair): Are there further nominations? Secondly, are there further nominations? Thirdly, hearing no further nominations, Mr. Lali is hereby appointed Deputy Chair.

Good morning, ladies and gentlemen. I would like to welcome you to this meeting of the Special Committee to Review the Personal Information Protection Act. My name is Ron Cantelon, and I'm the MLA for Nanaimo-Parksville. I will serve as Chair of this parliamentary committee.

Our committee has been asked by the Legislative Assembly to review the Personal Information Protection Act as per the act itself, which includes the requirement that every six years the act receive a review by a special committee of the legislative committee, an all-party committee.

We held a public hearing in Victoria on February 6, and today we have this public meeting in Vancouver. We've also received written submissions on the subject from individuals around the province. Today we have

a number of individuals who have preregistered to speak, but the space is still available if others wish to come forward and make themselves known to the Clerk.

Prior to hearing the first witness I would ask each member of the committee to please introduce themselves, starting on my left.

M. Polak: Mary Polak. I'm the MLA for Langley.

L. Krog: Leonard Krog. I'm the MLA for Nanaimo.

J. Rustad: John Rustad. I'm the MLA for Prince George-Omineca.

R. Cantelon (Chair): I would also like to introduce committee staff who are present here with us today. Everything that is said will be recorded and transcribed by our Hansard staff. On the left we have Lisa Coburn and Graham Caverhill. We're also joined by our researcher Josie Schofield and, to my left, Kate Ryan-Lloyd, who is the Clerk Assistant and Committee Clerk.

The committee has been asked by the Legislature to review the Personal Information Protection Act, and specifically the collection, use and disclosure of personal information by private sector organizations.

We are mandated by the Legislative Assembly to report back no later than April 19 of this year. At that time we will submit a report that will likely include the considerations of the committee and recommendations on how to improve the act itself.

The format of today's public hearing provides a total of 15 minutes to each presenter. This provides each witness with about ten minutes for their presentation and then allows a number of minutes for questions from the members of the committee.

I should also note that today's meeting is a public meeting, which will be recorded and transcribed by Hansard Services. A copy of this transcript, along with the minutes of this meeting, will be printed and will be made available on the committees website at www.leg.bc.ca/cmt/pipa.

In addition to the meeting transcript, a live audio webcast of this meeting is also produced and available on the committees website to enable listeners to hear proceedings as they occur. An archive copy of the audio broadcast will also be retained on the committees website.

Again, I'd like to thank you for coming and to thank the vice-Chair, who has just been appointed.

Mr. Lali, thank you for coming.

I see Mr. Greenwood is ready to present.

Presentations

G. Greenwood: Good morning. My name is George Greenwood, and for the past four years I have made it a personal interest to study the effects of identity and its various forms of abuse. For the last two and a half years I've been conducting open public seminars with the intent of teaching people to reduce their risks. Last August I had a book published called *In Your Good Name*. I only mention these points because they have

given me some background in being able to address the points I want to bring forward, of which there are two.

If I may, I refer to 4.3, principle 3, under "Consent." I propose the addition of the following, which I recommend as being 4.3.9: "A purchaser, when conducting business with a credit card, provides consent to the organization to use the information on that card in order to process the business transaction. The consent, however, does not include posting the full 16 digits of the credit card number, the expiration date, their printed name and signature on a receipt to be left for anyone to access."

In order to process this information, I believe that the numbers need to be truncated or left off that document entirely. As a personal comment, if I may, the current practice conducted by most restaurants, entertainment, hospitality and other service industries.... If I may use the phrase, I believe that it is private data suicide.

[0935]

As a second point, under 4.7, under "Safeguards," I propose the addition of what I refer to as 4.7.6:

"In the event of a breach, compromise or loss of data documents, either electronic disk, tape or paper, or any personal information in any format, either by theft or misplacement, the organization in question must inform the appropriate customers, clients, suppliers, employees or anyone personally affected by such a loss that their private or personal information has been compromised, leaving these people with the opportunity to place safeguards in order to protect their interests and vulnerability from either a personal or business concern."

Again, this is my personal comment. Simply, in a sentence, I believe if a business breaches my information, then I need to have the right for them to tell me that, so that I can protect myself.

R. Cantelon (Chair): Thank you, Mr. Greenwood. Do we have questions from the panel?

L. Krog: Looking at the final suggestion in the proposed addition — and I'm just being a little bit legalistic — I think it would be better to say "anyone who may be personally affected by such loss."

The reason I say that is.... This is presupposing that they will be affected. I think it's the potential — anyone who may fall into that category.

I happen to agree with you. I think that the amount of information we give out is incredible. I'm old enough to remember the promise made by the federal government when we brought in the social insurance number that it would never have to be used for any purposes other than dealing with the federal government. Of course, we all know what has happened as far as that's concerned.

G. Greenwood: I agree with that. I confess I do not come from a law background, so the individual words I appreciate any assistance with.

My point is to raise the fact that this is a danger area for the public, and I believe that it definitely has to be addressed.

H. Lali (Deputy Chair): Your 4.3.9 reference there on the document that you handed out and the truncating of the numbers. Personally, I agree with you there.

Most businesses will truncate the numbers except for the last four digits that are on there. But there are a lot of businesses that you deal with that will not, and the whole information is still available on that credit card receipt.

I'm just wondering: does your organization have any kind of data or stats or information regarding any misuse or theft as a result of this not being done — what you suggest? Do you have any kind of information that would actually help us?

G. Greenwood: Absolutely. If you'd like that, I have been in conversations with a young gentleman who was convicted of 23 counts of commercial identity theft. He tells about how these practices can be utilized and are utilized on a daily basis.

The fact of the matter is that when you go into a restaurant, most of us don't even pay attention to those slips that we sign, never mind understand what's on them. And when we leave that piece of paper behind.... In the drug trade on the streets right now, anybody that picks up that receipt that you have signed and put on the tip and such.... It's worth \$20 to any druggie on the street to go and turn that in to a dealer to be able to get that into the process of what we refer to as identity theft. It's absolutely huge, and most people don't even notice it.

To add to your comment, a lot of places do now voluntarily follow that practice, but it is just that — it's voluntary. I suggest that we follow the lead from the United States in December of 2006 where it was made mandatory by law that those 16 digits and expiry date would not be able to appear on that piece of paper that is put in front of a customer.

J. Rustad: Thank you for your presentation and your thoughts on bringing this forward.

I'm looking at 4.7.6. In particular, it could create some potential situations — for example, a cab driver that collects a credit card receipt. If he were to be forced to create a database of all of the individuals that he would come in contact with — build and maintain that database — and then have to be in a situation where if there was a breach that he found out about, he would then have to contact all those individuals.... You're talking about a pretty significant database that a cab driver would be required to keep.

[0940]

I'm a little concerned about that. Quite frankly, I don't necessarily want somebody like a cab driver to have me in a database that could ultimately be available for somebody to happen to steal a laptop or whatever the case may be and suddenly have a huge access database with regards to any particular information.

I like the idea that you have around it, particularly for the larger corporations, that if there's a breach of security of their information, a contact would help to be able to change that. But for smaller organizations, such

as even a cab operator or others, the logistics around it and the potential risk around it would be quite significant, I think.

The reason why I bring up that up in particular is, actually, I've had my credit card number.... I've tracked it down to.... I'm sure it came from a cab, because it was the only time that particular card was actually used within a two-month period. Somebody had stolen it and used it and bought a bunch of stuff on it. It created a whole fraud situation that I had to go through, and that was just over this past summer.

I like the ideas in terms of being able to have that contact information. But how would you propose safeguarding against a larger potential problem around the database?

G. Greenwood: I agree with you in the sense of an individual, a single operator — like that of a cab driver. But I don't see him.... Number one, he is not electronically kicking out a receipt for you to sign.

J. Rustad: Many of the cab drivers are doing that today. They have the technology where they scan the card and it actually prints out a receipt database that only has the last four numbers on it. There are still many cab drivers that have the old carbon-copy-swipe type of device, but more and more are now moving over to the newer technology.

G. Greenwood: Yes. I agree that there will be exceptions to this — there's no doubt about that — but I do believe that it needs to start somewhere. It does need to start going into the fact where.... You know, we could look at every possible scenario and turn around and say: "Well, it's easier just to ignore the situation." I do believe that it has to start somewhere, as I just said, understanding that there would be some exceptions. Perhaps the cab operator, as an example, could be that exception.

I'd just draw your attention to the next time you go to buy lunch, as a prime example. You will see that what I'm saying is there. It's so prominent that most of us just don't pay attention to it.

From the aspects of how it can be sold on the street, that information.... Once it gets on the street, who knows? Then it goes onto the IRC sites on the Internet and is being sold in Southeast Asia or eastern Europe or wherever it gets into the world system. Then you're in for the ride of your life at that point.

It needs to stop somewhere, and I see this as being a logical point of beginning to be able to start that process.

R. Cantelon (Chair): Thank you, Mr. Greenwood. I don't see any other questions.

I see at the bottom of your submission, Mr. Greenwood, itcanthappentome.ca. I presume that other consumers who are interested in your programs could contact you through that website. Is that correct?

G. Greenwood: Absolutely.

R. Cantelon (Chair): Okay. Thank you very much for a very informative and direct presentation. We will certainly take it under consideration. Thank you very much for coming today.

G. Greenwood: Thank you for allowing me to appear.

R. Cantelon (Chair): I don't believe we have any other registered witnesses available that have indicated they want to come, so we'll take a brief recess for about ten minutes to wait for the arrival of our next presenter.

The committee recessed from 9:44 a.m. to 9:56 a.m.

[R. Cantelon in the chair.]

R. Cantelon (Chair): We'll call the session back to order now and turn the floor over to Mr. Richard Gallagher from the B.C. Cancer Agency.

R. Gallagher: Thank you. I appreciate the opportunity to come and speak to you folks today.

I'm here on behalf of the B.C. Cancer Agency, particularly to try to draw the commission's attention to one or two aspects of the PIPA act, which I think, potentially, could cause difficulties in the future. I would emphasize that my presentation today on 21(1)(b) is not immediately urgent. I don't have a specific issue that I'm addressing it to, but I do want to draw your attention to this for the future.

The B.C. Cancer Agency presently has large programs in cancer research, trying to find the causes of cancer and cancer screening, attempting to diagnose cancer before it becomes obvious in its most preclinically curable stages. At present a parallel to 21(1)(b) in the FOIPPA act, which I know you folks are not sitting on today — that is, 35(a.1) — prohibits disclosure of information from public databases for research contact purposes. My understanding is that this was enacted as an amendment in 2003 to avoid the kind of abuses that might take place with people contacting individuals who were on government health databases.

Unfortunately, the unanticipated consequence of this has been that the use of these databases, such as the B.C. client registry, which was used to select "controls" — healthy, normal controls — for research carried out by BCCA, by the CDC and by university researchers, has unfortunately been disrupted, and in some cases projects have had to be given up.

I am, along with several of my colleagues, going to see the Hon. Olga Ilich, Minister of Labour and Citizens' Services, who the FOIPPA act comes under, but I would like to draw your attention to the fact that the same difficulty could arise with 21(1).

I'd like to illustrate this by just providing a couple of examples from our own work that we do. Most of you, gentlemen at least, on the committee are probably aware of PSA testing and the hubbub that that's created. We don't know yet whether PSA testing will actually reduce mortality from prostate cancer. However, there is a large randomized trial in Europe,

which should report in 2009, perhaps 2010, and this will tell us whether or not it does what we think it's going to do.

[1000]

Now, if that's the case, we will likely be mandated by the government to offer a provincial screening program, in the same way we do with Pap screening for cervix cancer and screening mammography for breast cancer.

Currently all PSA testing for screening purposes — that is to say, in asymptomatic men — is done by private labs such as LifeLabs, which used to be MDS Metro, and B.C. Bio, etc. If the most cost-effective way to mount such a provincial program for PSA screening was to actually ask the private labs to continue to do the primary screening, 21(1)(b) could have the effect of preventing the folks doing the primary screening from passing that information on and identifying information to the Cancer Agency for the purposes of follow-up and for the purposes of research on the effects of this sort of program on quality of life of men.

Example 2. I would bring up colorectal cancer. We know that screening using fecal occult blood in a test, which is actually run by commercial labs at the present time, is effective in picking up undiagnosed colon cancer.

Again, we have already received money from the provincial government to actually begin a vanguard program, if you will, for a colorectal cancer screening program for the province. Again, should the most cost-effective method of doing this include private labs continuing the primary testing, they would be unable to communicate that information to us for the purposes of doing research on the efficacy of this program.

With these examples, what I'm trying to indicate is that there are potentially some difficulties. We do realize that in any access to a database, privacy and confidentiality concerns are really of paramount interest. However, the kind of research that has been conducted using names from government databases and that could be conducted using names supplied by private firms, is safeguarded by the fact that each of these programs has to be reviewed and approved by a certified research ethics board — usually at the University of B.C., University of Victoria, Simon Fraser, etc. This provides, we feel, very good protection for privacy and confidentiality of individual records.

Again, I'm approaching the committee with the request that the committee consider a balance of the societal common good, which can occur from this kind of research and these sorts of programs, with protection of privacy and confidentiality.

In the section entitled "Why is Personal Contact Often Necessary in Health Research?" I've outlined three or four issues. I don't want to belabour those. Those you can read at your leisure. They relate mainly to methodological issues surrounding studies and to the fact that without proper response rates, study results can be so biased as to be invalid.

[1005]

The other thing I would like to draw the commission's attention to is that, in a parallel situation with

35(a.1) of the FOIPPA act, we used to be able to use government databases to approach individuals to act as healthy controls in our studies of cancer. Over the period from 1980 to about 2003 our unit alone actually contacted literally thousands of individuals. A recent request to the privacy group in the Ministry of Health about how many formal complaints had been made indicated that we'd had only ten complaints in close to 23 years of using this kind of facility.

Again, what I'm respectfully requesting is that you consider the possibility of altering 21(1)(b). I've provided two possible examples of how that might be able to be done — protecting confidentiality while ensuring that proper research can be done.

I think what I'll do is I'm going to leave it there and try to answer any questions you folks might have, in the interest of time.

H. Lali (Deputy Chair): Thank you very much, Mr. Gallagher, for your very thorough presentation.

People give their personal information with the knowledge and the hope that their personal information will not be shared with others or used in any way without their consent. What you're proposing to do is exactly what people don't want to have done with their information without their knowledge.

I'm just having a tough time trying to reconcile the two principles of protection of their personal information that they have provided. Yet you want to ask this committee to give the authority by making the changes to actually do exactly the opposite of what they hope will happen.

R. Gallagher: Let me clarify what I am asking, because I think that's an appropriate question to raise. We are not asking that any health information whatsoever on any of these folks be divulged to the Cancer Agency, simply contact information — that is, the person's name, phone number, address, etc.

The reason why we're asking for just that information is that, for the most part, the details and the information that we wish to seek from these folks is not information which is on government databases anyway. Secondly, people would in fact resent it if they felt that any health information was being divulged.

For instance, when we contacted individuals from government databases to act as controls, we included a sheet of information on how we got their contact data and the fact that no health information whatever had been divulged to us.

In effect, we are not asking that the Legislature compromise in any way in protecting the health information of people, simply that they allow us to contact people.

H. Lali (Deputy Chair): I'm not talking about the health information, but even their name, address and where they live is still personal information. The whole premise of the Personal Information Protection Act is to actually ensure the principle that people's information will not be accessed without their consent. Yet that's exactly what you are asking to be done, which in

my opinion — I speak only for myself — is contrary to the spirit of the act.

R. Gallagher: Again, I would draw your attention to the fact that prior to 21(1)(b) — 35(a.1) in the public act — we had contacted thousands of people with essentially no complaints about use of their contact information for what was considered to be legitimate research. In fact, most of them were actually glad to help us out with these studies when we contacted them.

[1010]

I understand why you wish to protect people's confidentiality and privacy. I'm simply asking that we try and balance the good that can come from research like this with the minimal information communication that would take place with this sort of change.

M. Polak: You just now touched on the delicate balance that the committee must strike in conducting the review. With respect to the issue of consent for the purpose of future contact related to research and the way in which you outlined it, could not the same result be achieved simply by making the request for consent for such a purpose during the initial contact?

R. Gallagher: If the labs thought about that and made that request, it could conceivably give us the information we need.

One of the things I would ask you to consider is that we'd be assuming, first of all, that this information would be collected routinely, and secondly, that it would be unbiased information in itself. Both of these are potentially open to question.

M. Polak: How would they open more of a question than the way in which you're suggesting it be done? In other words, given that you're only asking, as you say, for contact information.... I don't see the linkage you're drawing with the issue of bias.

R. Gallagher: If we're thinking in terms of a study — say, of quality of life and PSA screening — and only a certain proportion of the labs have actually asked men to sign for that....

M. Polak: Okay. Then you're not getting a true....

R. Gallagher: Unless that is policed by labs themselves — which, to be honest with you, they're unlikely to do — then we have a major bias in terms of the people that we can approach.

The other thing I would ask you to consider is that even in the event that we approach people, they can still turn us down flat for participating in any research. That does happen.

M. Polak: That brings me to my second question. You mentioned that the only thing you're really asking for is their contact details and that it doesn't provide the individual making the contact with any health information. No health information is disclosed.

In the case of the example you've cited around PSA testing, I would expect that in any health research, the very nature of the research being proposed would, in and of itself, indicate a connection between that individual and that particular area of research. In other words, if somebody's husband gets a phone call from XYZ research organization — "Hi, we're doing a research trial on PSA" — there's going to be some connection drawn from that.

I guess I'll put in the background for you to consider in your answer that, given the broad principles we have to consider, I don't know that the argument that says, "We're going to do good things with it...." Everybody that would argue that they want information would say that's why they want to do it. They want to do good things.

R. Gallagher: Of course, yeah.

M. Polak: How do you avoid making the connection with health information?

R. Gallagher: Historically, we have not made any assumptions about the names of folks that we have been permitted to contact. Usually what happens is that we send out a sheet describing the study — a sheet describing where their names were obtained from and the fact that we know nothing about their health status — with a request to participate if they qualify, and for a research assistant to call them.

[1015]

If people want to say no immediately or if they wish to participate immediately, we usually include a checkoff sheet in there. But, as most of us are familiar, we will tend not to use that sort of thing. Only about 10 percent of people respond that way.

So what happens is that a research assistant calls and says: "We're calling about the particular study of such-and-such. We'd like to ask you if you'd consider being a participant." If they say yes, we'll consider that. We then say: "We'd like to ask you a couple of questions."

M. Polak: So the qualification takes place post-contact as opposed to pre.

R. Gallagher: Yes.

M. Polak: You're not saying: "This is the right person for this study."

R. Gallagher: No, absolutely not. Again, as I say, no information is released to us about the individual — simply the contact.

L. Krog: I have to cheekily ask: when you made your request for the information about the number of complaints, was it a formal FOI request, or were you just able to ask for it and get it?

R. Gallagher: No. In fact, let me be honest with you. We'd been turned down for access to the database,

and I was interested in how many complaints.... I was doing a study of prostate cancer, and I was interested in how many complaints the ministry had had over the years from the 30 or 40 studies that we'd done. Ian Rongve, who is the person in charge of information access at the ministry, searched the database and told me it was about ten.

L. Krog: This leads me to.... I love taking contrary positions; it's my nature.

Just so I understand.... The necessity of you using this kind of data.... Given that the information you're requesting is a person's name and their address, in my community this is readily available in a phone book and in a mid-Island directory that even gives you the postal code if you want to mail them something.

R. Gallagher: Yup.

L. Krog: Why do we have to go through this process — requesting it through the Health Ministry, in a sense, or testing? In and of itself, to come back to Mary's point, obviously you want to ask people who have been involved with a health issue — that's the point here, right? — as opposed to just going randomly through the phone book.

R. Gallagher: Okay, that's a good question. For instance, if we're doing a case-control study, which is the kind of situation that this usually occurs in, there's something called the cancer registry. As you know, cancer is a notifiable disease. That registry is within our Cancer Agency, and we're mandated to use that to conduct research and to do surveillance and monitoring. So we actually know the folks who've been diagnosed with cancer. Again, with the material that we send out to them, we notify them that we got their name from the registry and that it's a notifiable disease, etc.

The reason we're interested in accessing large-scale databases like this is because of the changing demographics in our society. It's been estimated that about 20 to 25 percent of people no longer have a residential phone listing, particularly young people.

L. Krog: You don't have to tell a politician that, believe me. Trying to contact voters is impossible.

R. Gallagher: As that group comes into health issues, we're going to have a major difficulty getting good population-based responses to the research we need to do.

L. Krog: I must say that I think you've hit the nail on the head around something that's very important, notwithstanding what Churchill said about lies, damned lies and statistics.

Interjection.

L. Krog: My friend tells me it was Disraeli, not Churchill. Churchill claimed credit for it, of course.

I think that is what we face as a society — having that information available. I'm very glad you made your presentation this morning. I think it puts it squarely before the committee. Prior to you, Mr. Greenwood pointed out the misuse of personal information. That's one thing we have to balance, and on this side is something where you're literally talking about saving people's lives by making some information available so that the Cancer Agency and agencies like it can do their business.

R. Gallagher: I would emphasize that it's not just BCCA. The Centre for Disease Control, which is looking at infectious diseases, vaccination coverage and that sort of thing, is running into the same difficulty. They're unable to produce the information the government actually needs for effective vaccination policies.

[1020]

J. Rustad: Thank you for your presentation. I'll start off just by saying that I'm tempted, just on a first blush, to find a way where we can open this wide open in terms of research. When I look at the challenges facing our health care system and the challenges with cancer and with other things, the amount of research and the benefits that could come from research, from having access to wide databases, is phenomenal. It really is.

But the problem becomes the ethical issue of people's privacy and rights. That, of course, is ultimately what we're looking at here. I would think that if it were to be wide open, we might be in a situation where we'd be fighting some court challenges for many years to come around that whole issue. I'm often perplexed, because what's best for society sometimes is not what's best for individuals.

R. Gallagher: I recognize the dilemma you folks are in.

J. Rustad: That is a challenge. Having said that, sometimes bold action needs to be taken.

I do want to ask one question around this. With regards to databases, with regards to that information collected in research, do you draw a distinction between a private entity, a private company, wanting to do the research and have access to the information versus a public company, a Crown agency, wanting the information to be able to access for research — or even subsets on either side of the equation?

Then they become a challenge. I mean, no one trusts government, but fewer people trust private corporations when it comes to that kind of database of information.

What are your thoughts around that, and how do you draw that distinction? If you make the argument that if you're going to make a database available for research because it's in the best interest of the greater populace, where do you draw the line in saying, "Well, okay, but it can't go to a private corporation," when you can still make the same argument that with a private corporation, it's in the best interests of the general public for that research to be undertaken and hopefully find some solutions and answers?

R. Gallagher: That's a legitimate concern. Historically, I think that has been a major problem. Particularly, research conducted by pharmaceutical firms has drawn the attention of people to the potential for misuse.

The approach that I've made here has suggested that bona fide research is research which is passed by a public body, a research ethics board, as described in the tri-council guidelines. That relates largely to non-profit university, academic and health institutions.

J. Rustad: Just out of curiosity, though, I know a lot of research can start in universities and often gets spun off into the creation of companies or into other private companies. In essence, even though it may start in the public realm and the data may stay in the public realm, the benefits of it may ultimately go into the private. So you still have the same ethical dilemma around that.

R. Gallagher: Yeah. One of the reasons why I preceded my comments today with the kind of proviso that I'm talking on — I'm speaking today to non-clinical applications — is exactly that issue. Non-clinical applications refer to a screening in the public interest for cancer, research on epidemiology risk factors and causation of cancer.

To be perfectly honest with you, if we could.... The support within the private community of companies for that research is nil, essentially. One of the hardest things we have to deal with in studies is the fact that we need to raise all our money from bodies such as the Canadian Institutes for Health Research, the National Cancer Institute of Canada, the NIH.

There are, essentially, no private firms which support this kind of research, simply because it doesn't produce the patentable entities that can provide the profit that they need to drive their enterprise.

[1025]

J. Rustad: If we were to look at opening up, then we would need to create some sort of definitions around where those boundaries should be.

R. Gallagher: Yeah. It's interesting, because my colleagues and I have discussed this. I had assumed that my clinical colleagues would approach you folks, too, on this because there are some clinical issues concerning this information as well. I'll be honest with you. I just can't speak to you on those.

J. Rustad: Okay.

R. Gallagher: I don't treat patients myself, and I would be out of my depth speaking about that.

R. Cantelon (Chair): Thank you, Mr. Gallagher. We appreciate your submission and thank the panel for their questions.

R. Gallagher: Thanks very much for listening to me. I enjoyed our discussion.

R. Cantelon (Chair): I believe Mr. Darrell Evans is in the audience now for the B.C. Freedom of Information and Privacy Association. I'd like to invite him to come forward and make a presentation. You have 15 minutes. I suggest ten for your presentation and perhaps five for questions.

D. Evans: Okay. I would really like to thank the committee for making the effort to come to Vancouver and hear from groups such as ourselves. I know that at one point that wasn't considered, and we requested it. We really appreciate your coming across the ocean to see us.

My name is Darrell Evans. I'm the executive director of the B.C. Freedom of Information and Privacy Association. I'm also here representing the B.C. Civil Liberties Association. We work together very often on privacy and freedom-of-information issues. We're going to make a joint written submission to the committee from our two groups as well.

Just to give you a very quick background on the two groups. Our group, the B.C. Freedom of Information and Privacy Association — FIPA for short — is a non-profit society established in 1991 for the purpose of advancing freedom of information, open and accountable government, and privacy rights in Canada. We serve a wide variety of individuals and organizations through our programs of public education, legal aid, research, public interest advocacy and law reform.

The B.C. Civil Liberties Association was established in 1962 and is the oldest and most active civil liberties group in Canada. They are a group of citizens who volunteer their energy and talents to preserve, defend, maintain and extend civil liberties and human rights in British Columbia and across Canada.

First, I'm going to engage in a little bit of history. You folks were probably all around when the PIPA was debated and passed, but I think our role in it merits a little airing as well. The position we stated publicly is that the Personal Information Protection Act, PIPA, is a very good piece of privacy legislation.

In fact, it was a huge breakthrough for privacy rights in the provinces outside Quebec which, as you may know, previously had privacy law for the private sector. PIPA improved on the federal Personal Information Protection and Electronic Documents Act in several significant ways. It also fell short in a few, which I'll be discussing.

As you know, our act was required by the PIPEDA to be substantially similar to PIPEDA in order to be recognized by the federal government, and therefore, PIPEDA would not come into force here. It was found to be substantially similar.

B.C. showed strong leadership among the provinces in moving forward with this legislation in 2001 with an act that has real teeth. For this, great credit is due to the then Minister of Management Services Sandy Santori and to Chris Norman and Sharon Plater — whose names you have undoubtedly heard — the officials who conducted the public consultation and led the development of the legislation.

It was a product of a very thorough consultation process and a very fair one, we thought — even though I estimated about 50 business groups were heard from for every privacy advocacy group present, and there aren't too many of those. I'm not sure what the balance has been during this review, but I would be interested to find out.

[1030]

The consultation lasted about a year, and my group, FIPA, participated in 12 meetings with the government, by our count. I feel free to tell you now that what we saw when those consultations first started was not good legislation. It was a sketch, and we were not very pleased. As a matter of fact, we said: "What the heck is going on? This will never be substantially similar to the federal act."

We were cautioned by the government officials at that time that it was not a privacy bill. It was a data protection bill. The government officials wanted to lower our expectations at that time.

Just to give you an idea of what the difference between those is, a data protection law is about basically managing the government's personal information or, in this case, the private sector's personal information so that it's only collected, used and disclosed according to a set of rules to those who are authorized to access and use it. In this case the government and the bureaucracy and the businesses are firmly in the driver's seat.

Privacy legislation, as we consider it, is actually civil rights legislation. It has quasi-constitutional or constitutional rights of privacy which are enforceable, and the citizen is in the driver's seat. The citizen has actionable rights.

Data protection legislation like this bill is kind of a backdoor way of legislating additional civil liberties, civil rights for people, which is okay by us. It's sometimes a little misdirected but in effect.... Over the six months that we were involved in consultations with the government, we examined and debated progressive drafts by section — and, in fact, line by line.

A transformation began to occur by the end of that process. We were very pleased. In our estimation, the bill had turned into a serious privacy bill. Great credit is due to Chris Norman, Sharon Plater and the minister and the other officials in the government for doing this.

I'm going to say a few things about the positives of the bill, and then I'll get on to what we think could be improved. First, what FIPA likes about the bill. There are a few things I'll run through.

It's clearly drafted and simpler than PIPEDA. PIPEDA is kind of an awkward beast. It's got a schedule attached, which is the CSA code, the Canadian Standards Association model code, for the protection of personal information, and the interplay is very difficult sometimes. Instead, that was incorporated right into our legislation, and done very well.

PIPA covers the entire provincial private sector, including non-profit organizations such as ourselves, which we thought was only fair. Since we were lobbying for it, we weren't going to ask for an exclusion. That's not true in Alberta, as you may know. Non-

profits are excluded. But I think that may change, due to their own review. We'll see.

Our PIPA contains oversight and enforcement by a commission with order-making power, which is the biggest single difference between it and the federal PIPEDA, which we do not consider a good model. It's very confusing, I think, and fairly ineffective in some major ways.

The right of consent is at the heart of this law, which is as it should be. That's the primary principle behind privacy protection legislation. The exceptions to consent are fairly limited. The purposes for collection, use and disclosure must be specific and must be reasonable. "Reasonable" changes over time. It can go higher or lower, and we hope it continues to go higher, of course.

Consent must be explicit if information is sensitive. This is something we lobbied very hard for, and it refers, in effect, to medical legislation such as was just discussed. Consent for use of medical information must be specific, because that's more sensitive information.

What that really means is that there's such a thing as implied consent in the legislation. If it's obvious, you shouldn't have to ask for consent. The person is engaged in a transaction where you know that they're collecting your information. That kind of implication is not allowed for medical information. You must specifically say that you're collecting and using it, etc., and identify the purposes.

There is an exception allowing for use of personal information for research without consent, but it is fairly narrow. If you wish, I'll discuss the point that was just debated by your committee with the previous speaker.

[1035]

The access-to-information provisions are reasonable. That means the citizen's right to access to his or her information is pretty good, in that it's — another thing we lobbied for — a minimal fee. The word "minimal" is in the legislation. I don't know if that's in, for instance, Alberta's. It could have been "a reasonable fee," and who knows what that would have been?

There are no charges for access to one's own employee information. If I am an employee and I ask for my information, I don't have to pay for that.

It contains good whistle-blower protection. This was in the PIPEDA and not in the first draft of PIPA, to our great alarm. I said: "How can this really important facet be left out of the legislation?" It was put in, which we're very happy about.

There are strong penalties for offences, although there are a few offences, I think, that we will suggest should be put in. I won't go into that now.

How can the PIPA be improved? We think it can and should be improved with regard to several points, and I'll run quickly through those.

First of all, the exceptions to the principle of consent. As you know, the heart of privacy rights is that the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate. That's from the Canadian Standards Association code, and it's also in the PIPEDA. It's principle 1.

The exceptions and consent requirements in PIPA are, in our opinion, too broad. We will be proposing some amendments to remedy that.

Second, the openness of privacy policies and practices. This has become a big problem. Several people have made complaints and had to appeal to the commissioner to see privacy policies and had been refused. This refers to principle 8 of Canada's national standard model code for the protection of personal information, which is openness — meaning the requirement for organizations to be completely open about their policies and practices with regard to personal information. I can't underline this point enough.

Only when there is openness can the public give truly informed consent. If you know all the purposes and uses for which an organization is going to be using.... This is an area in which, as I say, the PIPA has been found wanting.

Some major complaints have gone forward stating that some organizations have been less than open about their privacy policies and practices, but the weak standard of PIPA has prevented them from receiving a written privacy policy or a thorough description of the businesses' practices. That's because, basically, corporations and lawyers found a way around the wording in PIPA, which we thought was fairly clear when you add them all up.

You've got to identify purposes — right? Are you going to do that over the phone? Some companies give information over the phone. That's it. They don't have a posted privacy code. So we'll suggest an amendment to remedy that.

Third, a limit to rights of access and correction. People must have the right to have access to the personal information request to be corrected where it's false. There is a problem with the sections of PIPA that apply to that — sections 23 and 24 — and we'll propose two amendments to remedy those shortcomings.

Fourth, offences and penalties. This has come up in the Alberta review, and we're basically chiming in with what the Alberta committee said.

First of all, failure to adequately protect personal information should be an offence. The public is very concerned about the security of personal information, particularly in cases where it makes them vulnerable — fraud and identity theft. These are skyrocketing, as I'm sure you've heard many times during your review. That will cause a failure of trust in the public in electronic transactions if adequate offences and safeguards are not put in. We will be proposing an amendment for an offence in that regard.

Second, the committee in Alberta found that destruction, alteration, falsification or concealment of evidentiary records should be an offence. That could be seen as being implied in the offence for obstructing the work of the commissioner, but that's not clear. We think it should be spelled out.

Fifth — and this is a very, very thorny issue: when personal information leaves Canada. As a society, we've worked very hard to create these privacy rights. We've had privacy legislation for the public sector

since 1983, and now we're rolling out with privacy legislation for the private sector. But there has always been a very annoying fly in the ointment in this regard.

[1040]

Here's the way I phrase the question. In an environment where personal information moves everywhere electronically and information management is globalized, how can we ensure that Canadian privacy law sticks to Canadian information, regardless of who has access to it or control of it? This is the thorniest issue of privacy today.

We can pass laws here, but what happens when our personal information leaves the country or in other ways becomes subject to foreign laws? As you know, this was a big issue with government information. The government was even sued over shortcomings in PIPA that would seem to have allowed access by American law enforcement to personal information. The government made a very strong series of steps to remedy that, which the court accepted. It's conceived now that there's a fairly good safeguard around our data.

One of those provisions, though, was that information could not be managed for a government-sponsored program outside of Canada. Obviously, this isn't going to be the case in the private sector, so what do we do? Do we disallow the contracting of management of information to companies that are foreign-owned? We'll be proposing some solutions that we hope will control that situation.

R. Cantelon (Chair): Mr. Evans, just to remind you that we have a clock on at 15 minutes. You've been 20, so I'd ask you to wrap up so that there is time for questions.

D. Evans: Have I? Oh my God. Terribly sorry. I'll wrap up very quickly, then.

The last and final item is privacy or security breach disclosure. You may know that the federal parliament is proceeding with legislation of this kind, or an amendment to PIPEDA, that will require companies to disclose when major security breaches have happened, and we will be proposing the same for this law.

On behalf of our two groups, I'd like to thank you very much and apologize for running so over time.

R. Cantelon (Chair): That's quite all right. We just have other people coming forward too. Questions?

L. Krog: Just very quickly. You are going to provide, I take it, a copy of your written submission today?

D. Evans: Sure. As soon as I clean this up, I'll give that, but also we will have a written submission for the committee.

R. Cantelon (Chair): Just in that light, Mr. Evans, next Friday is the deadline for written submissions, so I presume it'll be very detailed for us and very specific.

D. Evans: Right. We'll be rushing with that.

R. Cantelon (Chair): Thank you very much for your presentation. Seeing no other questions, thank you for coming forward.

The next scheduled group that we have is the Insurance Bureau of Canada. Mr. Corbeil and Mr. Lingard, if you would come forward. That's who I believe we have here today.

Just to alert the panel, we have another individual, Mr. Gibbens, who will be put on the agenda as well.

Welcome. The floor is yours, gentlemen. As we indicated to other presenters, 15 minutes. If you can do it in about ten, then we'll have questions.

S. Corbeil: Good morning, ladies and gentlemen. My name is Serge Corbeil, and I'm government relations manager for B.C., Saskatchewan and Manitoba with the Insurance Bureau of Canada. I'm joined this morning by Steven Lingard, who is IBC's assistant general counsel. Mr. Lingard works with our members on privacy law matters.

IBC is pleased to be here today to participate in your review of the Personal Information Protection Act, or PIPA. IBC is the national trade association representing the private general insurance companies that provide insurance for homes, cars and businesses.

Property and casualty insurers paid more than \$236 million in taxes in 2007 to the B.C. government and have \$7 billion invested in government and corporate bonds in B.C. In addition, our industry employs some 12,000 British Columbians.

IBC has been actively involved in the development of private sector privacy laws since the early 1990s. IBC and its members are strong supporters of the B.C. PIPA and the other private sector privacy laws in Canada — namely, the federal privacy law and the provincial laws in Alberta and Quebec.

Property and casualty insurers have long appreciated the need to protect the personal information of their customers and other individuals with whom they deal in the course of handling insurance claims. IBC and its members were active participants in the B.C. government's initial consultations on the development of PIPA, and we will continue to be actively involved in consultations on this important law.

As you know, the federal and Alberta private sector privacy laws are also undergoing statutory reviews, and IBC has made written representations on all three reviews. We filed a letter with the Clerk of your special committee on February 6, and a copy of our submission, I believe, has been distributed to you.

[1045]

This morning we would like to discuss two of the issues from our submission to your committee. I will now ask Mr. Lingard to discuss these issues.

S. Lingard: Good morning. My name is Steven Lingard, and I am assistant general counsel with the Insurance Bureau of Canada. The first issue I would like to address is privacy breach notification. I would like to preface our remarks by first commenting on the leadership role of B.C. Information and Privacy

Commissioner David Loukidelis and his office. Commissioner Loukidelis and his office have played pivotal roles on such key issues as transported data flows; international privacy efforts, such as the APEC privacy framework; and privacy breach notification.

On the issue of privacy breach notification, Commissioner Loukidelis's office took the lead in Canada by preparing, in December 2006, a guideline entitled *Key Steps for Organizations in Responding to Privacy Breaches*. These key steps were supplemented by another document, a breach notification assessment tool which was developed jointly with the Office of the Information and Privacy Commissioner of Ontario.

These two privacy breach guidelines were subsequently adapted by the Office of the Information and Privacy Commissioner of Alberta and the Office of the Privacy Commissioner of Canada.

IBC's members support the four-step approach outlined in the *Key Steps* guideline, which are: contain the breach, evaluate the risks associated with the breach, notify the affected parties as necessary and prevent future breaches. In our view, these key steps provide a clear and workable approach to dealing with data breaches and the associated risk of harm to individuals.

We believe that these guidelines should form the basis of PIPA's approach to addressing this issue and that the B.C. government should allow organizations sufficient time to work with these *Key Steps* guidelines and to gain valuable experience in effective means of handling breach notification.

Privacy breach notification may sound like a simple task, but it is actually a complicated procedure that must be done properly. Organizations — whether they are small, medium or large — will need to review their privacy and information security practices from the perspective of how to respond to a privacy breach.

Organizations will also need to review their outsourcing arrangements with other organizations so that if the breach is caused by the organization that is providing the outsourced service, there is the appropriate coordination of efforts to contain the breach and notify the affected individuals.

If the B.C. government decides to proceed with the legislative approach, we suggest that the government consider a legislative provision that would require organizations to establish, by a reasonable date, policies and procedures consistent with the purpose of these privacy breach guidelines.

If I can just pause at this moment, Mr. Chair and committee members. Our speaking notes this morning are not our exact written submission that we sent to the committee. We can provide you with a copy of our speaking notes later, if you'd like. I'm just trying to pick on two issues from the six or seven we mentioned in our submission.

Our second issue is an insurance-specific issue — namely, witness statements. A simple witness statement presents serious problems which were not considered by the legislative drafters of PIPA. P-and-C insurers have a contractual obligation to defend their policyholders against claims that are made against

them. In the course of investigation and settling insurance claims, P-and-C insurers are often required to obtain witness statements from people who saw the incident or who have information that is necessary for the investigation of the claim.

It is to the benefit of everyone — policyholders and those individuals who are making insurance claims — that all of the relevant facts and information about the incident are gathered by the insurer as quickly and accurately as possible. As a practical matter, in some cases witness statements must be obtained even before a claim has been formally made to the insurer and before the identity of the claimant has been established.

A witness statement may contain different types of information, such as the individual's observations of the facts of the incident, information about another individual who was involved in the incident and information about the individual who's giving the statement.

[1050]

PIPA requires an organization to obtain the individual's consent before collecting and using their personal information. There are limited situations where personal information may be collected and used without consent. PIPA also requires an organization to give a person access to their personal information and to correct inaccurate information.

Now, the witness statement is given voluntarily by the witness, so the witness consents to giving the statement. The witness can obtain access to their personal information in the statement. However, there is uncertainty about the position or rights of the subject of the witness statement.

Before I proceed further, let me give you an example of a typical witness statement. John Smith slips and falls on the walkway of Jane Brown. Smith makes a claim against Brown for his injuries. Brown notifies her insurance company about the incident.

The insurance company needs to gather information about the incident. A neighbour, Tim Black — notice these clever names — saw the incident and gives a statement to Brown's insurance company. In this example Black is the witness. He saw what happened. Smith, who slipped and fell, is the subject of the witness statement.

If I can go back to PIPA, Smith, who is the subject of the statement, asks the insurance company for access to the witness statement. He asks to have the statement corrected because he says that the personal information in it about him is inaccurate. He also withdraws his consent to the use by the insurer of his personal information in the statement. But he still wants his insurance claim to be settled.

The insurer is caught in an untenable situation, where the claimant is using PIPA to prevent the insurer from using the witness statement to determine the facts of the incident and to settle the claim. In our view, it would be unreasonable to prevent the insurer from collecting and using all of the relevant facts about the incident in order to adjust or settle the claim. If a lawsuit is commenced by the claimant and the matter proceeds to trial, it would also be unreasonable to

prevent the court from having available to it all of the relevant facts related to the incident.

It is uncertain whether the subject of a witness statement has a right under PIPA to prevent an insurer from using the witness statement on the basis that their personal information was collected without their consent. This situation would have serious negative consequences, as it would effectively allow an individual, the subject of the statement, to prevent another individual, the witness, from reporting what they saw or heard and would prevent an insurer, and by extension the court, from hearing all of the relevant facts about the incident.

A witness statement may as easily confirm and verify the claimant's version of the events as it might cast doubts about the incident. An insurer must be able to collect and use all of the necessary facts about the incident in a reasonable manner, including obtaining statements from witnesses without the subject's consent.

Our written submission to this committee includes recommendations on how to resolve this problem, but we know that there is no easy answer to this issue, which relates to the principles of consent and access. Assuming that this committee agrees that this matter needs to be considered further, we suggest that as a next step the committee consider a recommendation similar to that in the federal government's response to the PIPEDA review — namely, that there be consultation on this issue with the Privacy Commissioner, the legal community and other relevant stakeholders.

S. Corbeil: This morning we have briefly summarized two of our issues and proposed some solutions and recommendations. We would be pleased now to answer any questions that you may have on these or any of the other issues that are in our written submission.

M. Polak: I'll start with the second question that I had, which is the page I'm on. On page 6 of your written submission you discuss the difference between a minimal fee and a reasonable fee. The Alberta legislation allows for a "reasonable fee."

I guess my first question is: have you encountered circumstances wherein the term "minimal fee" has resulted in members having to curtail a fee that they've determined, in their minds, was reasonable based on the work they had to do?

[1055]

S. Lingard: Yes, we have. This actually is an issue not only for the B.C. PIPA but for PIPEDA as well, in that, in reviewing an insurance claims file.... Please bear in mind that a claims file can be a small file, or it can be a very large file. It's very different from if you buy a carpet from the Hudson's Bay Co., where they have a one-page document on you. An insurance claims file can be many inches thick.

To review the claims file to determine what information should be provided is more than an administrative procedure. It will require someone with some legal training to review the file. A minimal fee.... My understanding is that it's been interpreted as being basically

photocopying. It doesn't allow the insurer or any other organization to make an argument or submission to the Information and Privacy Commissioner that in this situation, given the size of the file, it would be reasonable to allow the organization to also include in the fee some of the time of the person involved in reviewing the file.

Yes, it is an active issue.

M. Polak: Second question is related to page 4 of your written submission. You've talked about — at the very bottom — "add clarification in PIPA that when litigation has commenced, the provincial rules of civil procedure should govern and prevail over the access provisions in PIPA."

If that type of action was taken with respect to altering or amending PIPA, would that not cover off many of the other aspects of the request you're making with respect to witness statements, etc.?

S. Lingard: Yes, it would. Also, the clarification about litigation privilege. Litigation privilege is common law, but it's not very well understood. People know solicitor-client privilege.

Getting back to your specific question, yes, it would. A lot of these issues are related. We've come up with some possible solutions, but we are aware that for every solution, there might be a weakness to it or a drawback. We're not saying that this is the only way. Some of these issues do overlap.

But yes, to ensure that the provincial rules of civil procedure would govern a matter would address a number of our issues. I can see other committee members are putting their hands up. There must be some interest.

J. Rustad: Actually, I wanted to talk a little bit about the privacy breach notification. The issue was brought up earlier by another presenter. I want to put the same question to you as I did to the other presenter.

Where do we draw the line between companies' requirement to keep a database of information, and then to be able to notify people within that database if there is a potential breach, versus the risk associated with companies keeping a database of information and the possibility of that database getting out as a leak?

I'm thinking not so much of the larger corporations or government agencies but smaller companies, such as a corner restaurant, coffee shop, cab driver — those sort of things. Where do you start drawing that line of information and the notification of potential breaches — like I say, as well as the security of that information?

S. Lingard: That's an excellent question, and I'm just sort of thinking through some possible answers.

First of all, you'd go back to the first premise that an organization should only keep information that it needs and should only keep that information for as long as is necessary. That would alleviate the possibility not of a risk but of a breach. If a breach happens, then it would affect a smaller group of individuals.

I think some of the privacy breaches have shown that some organizations have held onto a lot more information than they need. They should have gotten rid of the information.

You mention the example of a small organization. I think you mentioned the example of a corner restaurant.

J. Rustad: It could be something more like maybe a smaller department store that has a client base and that keeps their billing information on record so that when a customer comes in, they can customize what the product is that they may buy.

Where do you start to draw the line of size, I guess?

S. Lingard: What is being discussed at the federal level, and I know in discussions with Alberta and B.C., is that there be thresholds to determine the sensitivity of the information and whether there's been serious injury or loss to the individuals affected.

[1100]

It would depend upon the type of information. It would depend upon how much information is lost.

Now, the loss of information to six people is as important to those six people as would be a data loss to a million people. The difference would be how the organization would respond, what it would need to do. It's easier to respond to six people and tell them about it than it is to a million people.

I apologize if I haven't answered your question exactly. I'm still sort of thinking through the various scenarios that you've given. If you care to ask another question or follow up on it, I'd be pleased to continue.

J. Rustad: Maybe if you could give some thought to that. I think the Chairperson mentioned that next Friday is the deadline. If you could put some thought to it and maybe provide us with something by then, that would be much appreciated, in terms of where some of those lines may be or what some of those regulations, if you want to put it that way — how they would have to be defined.

S. Lingard: Yes, we will.

L. Krog: Back to page 4, the recommendation that Mary brought up, adding a clarification that the provincial rules of civil procedure would govern and prevail over access provisions once litigation has commenced.

Do you see the possibility of either encouraging or discouraging litigation as a result of that recommendation? And how do you reconcile those?

S. Lingard: I don't think it would discourage litigation. I think that once a matter goes to court, the rules of civil procedure have governed what information is accessible and how it's being used. That's gone on for centuries.

PIPA is a new law, as is PIPEDA. They're complementary, so I don't think it would discourage litigation. I think that the litigation system in place works fine. It allows the judge to make the determination of what

information is relevant. There are affidavits of documents, so information is exchanged or disclosed. It allows the judge to determine the credibility of the witnesses.

It's more of a face-to-face situation, where more factors are considered than simply under PIPA, which is a paper-based solution. I don't think it would discourage. I think it would clarify the situation.

R. Cantelon (Chair): Gentlemen, thank you. You've raised a very substantive issue that's going to require some analysis by members other than this committee, as you refer to the legal community. I'm sure it will get the attention it deserves in our consideration and as we move forward with recommendations. Thank you very much for coming today and for your submissions.

S. Corbeil: Thank you. We'll be following up.

R. Cantelon (Chair): Now I'd like to ask Anne Landry to come forward. I would acknowledge and appreciate that Ms. Landry has come here at no small trouble and personal expense, from Alberta, to make a presentation to us, as I understand she did as well to the Edmonton equivalent of the PIPA committee.

A. Landry: Yes, I did. Thank you.

R. Cantelon (Chair): Thank you for travelling so far to make your case to us, and you're welcome. You have 15 minutes to make your presentation, so please proceed.

A. Landry: Thank you, Mr. Chair and hon. Members of the British Columbia PIPA review committee. I greatly appreciate the opportunity to present before you today.

I present as an individual Albertan with over four years of experience using the Privacy Act processes under the Alberta Personal Information Protection Act, PIPA, and under the Alberta Freedom of Information and Protection of Privacy Act, due to my employment as an investment specialist trainee with ATB Investor Services, ATB Financial, for five months in 2003.

I currently live in downtown Calgary in the constituency of Calgary-Buffalo. In the 1990s I lived in Vancouver in the constituency of Vancouver-Point Grey, the current constituency of the Hon. Gordon Campbell, Premier of British Columbia.

It is my hope that my experience will be helpful to you in formulating legislation to better protect the rights of individuals under the British Columbia Personal Information Protection Act. I presented before the Conservative-dominated Alberta PIPA review committee in Edmonton, Alberta, on May 1, 2007, and my presentation is available at the transcripts link for May 1, 2007, at the Alberta PIPA review committee website — www.assembly.ab.ca/pipareview/default.

The recommendations proposed in the final report of the Alberta PIPA review committee ignore my recommendations and are apparently very harmful to

the rights of individuals at a time that apparently few individuals in Alberta are aware of their rights or of the one-and-a-half-year-long Alberta PIPA review process.

The final report of the Alberta PIPA review committee that was tabled in the Alberta Legislative Assembly on November 14 can be obtained at www.assembly.ab.ca/pipareview/report/finalpipareport111407.pdf.

[1105]

Contrary to the terms of reference, no preliminary report was first issued to the public for review. Consequently, the final report of the Alberta PIPA review committee should be disallowed, pending involvement of the public — the hard-working individual Albertans who constitute the Alberta advantage and whose rights Alberta PIPA is to protect.

After much unexplained delay, I have just recently received Alberta OIPC orders regarding my three inquiries involving my information as held by ATB Investor Services and ATB Financial, a Crown corporation of the Alberta government, and by the national registration database and the Alberta Securities Commission, the Alberta provincial securities regulator.

These orders are available on the www.oipc.ab.ca website and are F2006-005, F2006-022 and F2006-017. These Alberta OIPC orders constitute an outrageous denial of my basic rights and apparently set precedents that will harm many in Alberta, British Columbia and elsewhere in Canada.

These three Alberta OIPC orders are apparently orders of opportunity — orders that would apparently fail under judicial review for the apparent lack of carelessness and/or correctness and/or reasonableness and/or fairness and/or objectivity and for failing to be rendered within 90 days of my request for inquiry, but that have nevertheless been rendered at a time when it is well established that I cannot afford three judicial reviews, each at approximately \$15,000.

The problem is the apparent lack of accountability of enforcement bodies and the apparent assault on the basic democratic rights of individuals in Alberta that result in the apparent lack of safety of personal information, including information regarding investments. Legislation that should protect the rights of individuals is now apparently being used to strip them of their rights of access to, completeness and accuracy of, confidentiality of and security of their own personal information — information that individuals own title to.

As a result of the apparent absence of basic democratic rights for individuals in Alberta, (1), employees can be fired for ongoing performance concerns in response to valid requests regarding their own information. Then not only are individual Albertans denied protection under section 58 of Alberta PIPA, "Protection of employee," but they are also arbitrarily disintitled to their information by the Alberta OIPC on the basis of the litigation context, wrongful dismissal nature of the dispute.

This is despite the fact that no clause exists in Alberta PIPA that allows an individual to be denied rights to his or her information on the basis that the information apparently proves the apparent wrongdoing of the organization.

(2) Salespeople can be fired on the basis of having difficulty with sales at a time that they are actually clearly excelling at sales as objectively measured by sales pipeline performance management reports. Then the objective facts regarding their sales performance can be denied to them not only on the basis that such information is considered work product and therefore not their personal information, but also on the apparent basis that employees are now apparently only allowed access to opinions or rumours regarding their performance but not allowed access to the factual information that objectively establishes their performance.

(3) Investors can be indefinitely denied access by their investment dealer to their own know-your-client, client account agreements at a time when individuals are raising concerns regarding incongruities involving their investments. This is despite the documents themselves in securities legislation, policies and rules that clearly reveal the individual's entitlement to these documents as their personal information.

The recently translated June 14, 2006, judgment regarding the case of an elderly couple in *Markarian v. CIBC World Markets Inc.* in Quebec Superior Court, at www.investorvoice.ca, reveals the need for investors to have legislated immediate access to their investment documentation to protect themselves from reprehensible conduct, including fraud, that is knowingly perpetrated by dealers against vulnerable individual investors.

(4) Investment advisers can be abruptly terminated in apparent response for appropriately forwarding the know-your-client investment instructions of customers. The same investment advisers can subsequently be denied access to their security compliance information, information about an investment adviser that would reveal apparent wrongdoings of the dealer.

The well-publicized case of Carolann Steinhoff — a very successful broker from Victoria, B.C. who was wrongly accused of wrongdoing, which took several years and much expense to exonerate her from — illustrates the need for investment advisers to have legislated, immediate, without-delay access to and completeness and accuracy of their own securities compliance information. The Carolann Steinhoff case is also documented at www.investorvoice.ca website.

[1110]

(5) Investment advisers can be arbitrarily denied access to, completeness and accuracy of, and correction of their information in the national registration database despite securities legislation multilateral instrument 33109 that states that "information in the NRD is the individual's personal information" and that "this information must not only be true and complete but be supported by documentation that is retained for seven years by the dealer."

The harm. I've spoken of the harm that has occurred to me due to the lack of rights under privacy and securities legislation in Alberta during my May 1, 2007, presentation to the Alberta PIPA review committee. At this time I stated: "My career, my finances, my health and my personal life have all been severely

negatively affected. Several times I have been on the brink of bankruptcy, and I am now over \$100,000 in debt. I was unemployed for most of two years and have now also apparently lost my new-found career in the financial investment services industry. But for the grace of God, my family and those who came to my aid, I would now be on the streets."

More than four years since my direct request to ATB, and despite more than four years of Privacy Act processes at taxpayers' expense by the Alberta OIPC, I still do not have that which I have long sought, although I have demonstrated the existence of the documents that I seek and they're in the binders you have now.

ATB's approximately 4,100 employees, and other employees, may be interested to know that I still do not have access to nor completeness and accuracy of my information regarding my performance as objectively measured by the investment specialists accountability profile that constituted my performance description, and that I still do not have confirmation of my sick days off that was important to establishing that I was sick and unable to work and receiving short-term disability payments from ATB at the time ATB abruptly terminated me. Nor have I been informed of the outcome of any investigations by the Alberta OIPC of the serious breach of security, of personal information involving ATB Financial and its pension administrator, which I was informed of by ATB in October 2006.

ATB's approximately 600,000 customers and other investors may be interested to know that I still have not received from ATB the ATB investors' services know-your-client information, including my know-your-client account agreements regarding my RSP mutual funds held through ATB investor services that were involved in the circumstances of ATB's abrupt termination of me.

The solution. The solution involves a radical overhaul of the privacy and securities enforcement systems in Alberta as well as elsewhere in Canada. Existing provincial privacy and securities enforcement systems are not working and need to be scrapped. Similarly, the self-regulatory organizations — the Mutual Fund Dealers Association of Canada and the Investment Dealers Association — should be scrapped. No organization should be elevated above the law.

Privacy and securities legislation enforcement bodies should be provided with the legislated ability to award substantial fines to organizations for their failure to comply immediately with valid direct requests of individuals. These fines should be awarded to the individual who has suffered from the lack of compliance with his or her direct request. Similarly, substantial fines that are also payable to the individual should also be levied against enforcement bodies for failure to appropriately administer and enforce legislation.

I will be providing this presentation that I'm making today and the supporting materials on the following website: www.investorvoice.ca/cases/broker/landry/landry_index.htm.

R. Cantelon (Chair): I presume that you understand that all written submissions — I think you've

given us a considerable amount of material — need to be done by next Friday.

A. Landry: Yes.

R. Cantelon (Chair): So simple reference to a website wouldn't necessarily comply. If you want anything forwarded to us, please make sure you forward it to us.

A. Landry: Thank you. What I mean is that I've provided you with a binder of information today and also a 35-page report. It will be on that website. That's what I'm referring to.

And I haven't even touched any of the exhibits. They show the circumstances of the case of what I've just mentioned right now.

L. Krog: As I hear you — and I appreciate the time is tight this morning — the thrust of your presentation is that the fining provisions are not sufficient to ensure compliance with requests, essentially. I'm trying to simplify it very much, but that's the thrust of what you're saying this morning.

[1115]

A. Landry: Exactly. The rights of individuals should be documented specifically in the legislation to state that the right is a right regarding a direct request and that failure of organizations to comply with access, completeness and accuracy, consent, security — every aspect of the law — upon a direct request will result in penalties. Otherwise, you get the situation that I have found myself in. Four years after my direct request I still do not have the information that I sought.

Then also, right now the legislation.... For example, section 59 of Alberta PIPA does specify offences and penalties. A clear indication of the lack of enforcement is that over the past four years there have been no fines implemented, and organizations, I believe, note that — how easy it is. There is a value to information. That value is at the time of the request, not four years later.

You will see in the binder of information I provided you that I'm not just the only one noting the lack of enforcement in the privacy and securities industry. It has been well reported in the media and is a concern that's being addressed right now at the federal level in terms of a new securities organization.

I think that in terms of your legislation, you can lead in making changes to protect the rights of privacy of individuals. I've given you documentation regarding the recommendations made by the Alberta PIPA review committee. In my 35-page report under the exhibit of the PIPA review committee final report, you'll see that the amendments actually strip away the rights of individuals to their information.

I spoke in the May 1, 2007, presentation regarding some of these amendments. For example, there's an amendment to allow the Privacy Commissioner not to make an order. If there's no order, that's lack of

accountability. It can sweep under the table anything without addressing it. If there's no order, there's no way for an individual to appeal or go to judicial review. If there's no order, there's no way for an individual to claim damages under section 60 of the act.

Another very damaging amendment is the setting of a limitation on the prosecution of offences. In the final report of the Alberta PIPA review committee you'll note that it mentions that currently in the Alberta PIPA there is a six-month limitation on the prosecution of offences. There is no limitation currently. To set a two-year limitation is to encourage organizations to commit offences and then delay indefinitely regarding that. Also, it's much to the harm of the individual. So I would recommend setting absolutely no limitation on the prosecution of offences.

Thirdly, another of the amendments that I spoke against was the issue regarding security breaches. The amendment that has resulted makes it not mandatory for organizations to report breaches of security to an individual. It sets the Privacy Commissioner up as an intermediary. Doing so only allows breaches of security not to be reported.

Not only is it important to report security breaches to the individual, but it's important also to report it to the Office of the Information and Privacy Commissioner and then to have the Privacy Commissioner investigate and report.

I was informed in October 2006 of a serious breach of my personal information by ATB in regards to social insurance number, name, birthdate and other information. I have not heard back from either the ATB or the Privacy Commissioner since. If I had not gone to the Vancouver 2007 conference on September 20 and 21 and found myself sitting next to the privacy representative from ATB at one of the security conferences, I would not have determined that the information is apparently still lost and I am just expected to somehow deal with that without knowing what has become of the issue.

Also, this breach occurred, possibly, in October 2006, and I haven't been an employee of ATB since 2003. I wasn't subject to pension at that time, and the information seems to have been breached by their pension administrator. A key question for me is: why is my information even with the pension administrator at this time, three or four years after?

I don't want to end up in the situation where I walk home and open my door one night, and someone else is there claiming to be me. I would like someone to take this on in a proactive manner and inform me of the result of any investigation by the Alberta OIPC into this.

[1120]

There are also other amendments that are very harmful, as well, to the individual rights in that they are changing the standard in terms of correctness — instead of being "a reasonable person," which is the standard under section 2 of Alberta PIPA, to being what an organization would consider to be reasonable, which is not appropriate. The standard in law is what a reasonable person would consider to be reasonable,

and that is what should be left. It shouldn't be left to be decided according to what an organization would consider to be reasonable, because an organization typically is considering oppositely to what an individual would.

Also, they are amending Alberta PIPA, apparently, to make it such that if you have information that is embedded in a record of information, you are not going to be able to access it. It's the small nuances of wording — information versus records of information. It's listed as a minor technical amendment in submission 63 by the Ministry of Service Alberta that oversees the Alberta OIPC, but that apparently is what the effect is: to disallow individuals access to their information.

In relation to me, how that would affect me is that my sales pipeline reports.... For example, I was an investment adviser, a representative salesperson. There are insurance salespeople, real estate salespeople and salespeople all over who are managed by their sales performance reports. On those reports there is customer information. I would be able, under PIPA, to have my own sales successes — my total sales for the month or whatever — extracted so that I know how I am performing to target. Under this new amendment, apparently, of just allowing records of information, I would not be allowed that.

Order F2006-005 disallows salespeople access to their sales pipeline reports. It also disallows individuals who have been wrongfully dismissed from using the facilities of the Alberta Office of the Information and Privacy Commissioner — which is most damaging, because that encourages organizations simply to terminate individuals in response to their requests. Then they do not have any right to use — apparently, under this F2006-005 — the ability of the Office of the Information and Privacy Commissioner. What needs to be done is to have greater accountability of enforcement organizations.

R. Cantelon (Chair): Well, once again, we appreciate all the information that you've given us. You've highlighted many concerns for us, and I thank you for the time and expense you've taken personally to come here and make this extensive presentation to us. Thank you, Miss Landry.

A. Landry: Thank you. I greatly appreciate it.

R. Cantelon (Chair): I'd like to call Mr. William Gibbens to come forward.

W. Gibbens: I must say that I'm very appreciative of the committee for hearing me on short notice. I had planned to come to one of your hearings in Victoria and was unable, due to professional commitments. It so happened that on short notice I was downtown today and saw this advertisement in the paper.

R. Cantelon (Chair): Please proceed.

W. Gibbens: I did a bit of a review of the act the other evening. What I find as a layperson is that it's

fairly complex to interpret intraorganizational relationships. In my experience as a member of the public, what is more complex about the act and what is really not clearly addressed is the relationship between private organizations — be they profit-making, non-profit or professionals acting as professional corporations — and government, be they a ministry such as the Ministry of Health or a health authority such as Vancouver Coastal Health, Fraser Health Authority and so forth.

Now, in our everyday lives, our business relationships and the information we exchange formally and informally are actually quite complex. What I find lacking in the act is a lack of controls, of checks and balances on information-sharing between private organizations and government. When that falls apart, it endangers — in the case of medical and health information — the life, health and safety of members of our community and the integrity of government institutions in the province.

[1125]

Essentially, when you've got government bodies or you've got boards of directors, for example in the case of a health authority, you have senior executives and you have employees. Some of these employees or executives may also be professionals and may also be providing services and billing the health authority or be in an employment capacity or other executive function.

My experience in having a loved one in care in this province is something I wouldn't recommend to anybody. But I did have some dealings with a private organization known as the Caregivers Association of B.C. What I found was that there was an informal relationship between the Caregivers Association and one of our health authorities and that our health authorities were also providing services to me as a family caregiver. I was offered complete privacy of my personal information by the health authority.

I found, however, that a senior official working at the board level had direct access to my personal information within the health authority for services rendered to me as a family caregiver. That senior official was also giving direction to lower-level employees, professional employees such as social workers, to exchange information with a private organization called the Caregivers Association of B.C.

In addition, a renowned physician not only of a private corporation but also a medical director of five hospitals under the health authority, was medically billing the health authority for professional services, also billing another family member for a medical assessment affidavit in B.C. Supreme Court and also on the board of directors of that private Caregivers Association of B.C.

I found, when that affidavit was seriously questioned in B.C. Supreme Court, that I was kicked out of the caregiver's support group of Vancouver Coastal Health Authority, denied a course that I'd been on a waiting list for, for a year and that I had been registered in. I was kicked out of the course. I was denied registration in a Caregivers Association of B.C. open public forum.

At the same time, I discovered that some secret funding had been provided for the Caregivers Association of B.C. by the Ministry of Health. Of course, one of their key principles is that they want to be "useful to the ministry." So I called the ministry and was told to make a FOIPPA request. That was in 2006. I only recently discovered that they received \$300,000, which was kept secret for a number of years because the government was claiming there was absolutely no money for such funding.

However, that ministry official revealed the fact that I'd discovered the secret funding and I was then denied access to my loved one in a private care home in the province of B.C. with the involvement of a senior official of the health authority.

R. Cantelon (Chair): Mr. Gibbens, may I...?

W. Gibbens: So we're talking about very serious and complex situations that this act does not appear to be able to address.

R. Cantelon (Chair): I just wanted to interrupt you, because if you have specific questions, I want to first mention to you, caution you, that everything that you're saying is a matter of public record.

W. Gibbens: I understand that.

R. Cantelon (Chair): And I hope you appreciate that. If your complaint basically is a specific nature as to how you were treated, there are other ways to seek redress, among them the Ombudsman. This committee is not here to redress personal issues. This committee here is to understand and receive specific recommendations towards the PIPA act itself. So if you could focus on that.

W. Gibbens: I'm trying to move on to that, actually.

R. Cantelon (Chair): Okay.

W. Gibbens: I don't wish to dwell on the facts. What I do wish to say is that there appears to be no coverage of conflict of interest within the act. In other words, a person who is on a board of a private organization might also be retained by government — employed by government and billing government — and know extremely personal information about individuals who are a member of that organization or who might wish to join.

[1130]

So the act, I think, falls very short in addressing questions of conflict of interest. While it does address matters of providing information to government or policing agencies for the purposes of investigation and this type of thing, which any reasonable person might understand, the act does not address informal information exchanges, does not address direction being given

by government to private organizations who are in fact beholden — if they're non-profits and seeking government funding or funding from health authorities — to them for their funding.

These, I think, are very serious matters. Most members of the public don't look at privacy as a very serious issue until they come in like I did today and hear the Insurance Council talking about serious matters and hear investment people talking about how complex and how troublesome it can be. In our particular case, it's a matter of no small high drama, but people's lives are at stake.

You are legislators. I believe this act needs a very serious review with regards to relationships and information exchange between private and either commercial or non-profits and government bodies in any form. I believe this act must address issues of conflict of interest related to boards of directorships, professional activities, employment activities and, where it crosses the line, between involvement with government and private organizations and where the funding comes from. Those are two things that I don't think are adequately addressed within the act.

I'll give you a few minutes to ask me some questions.

R. Cantelon (Chair): Thank you, Mr. Gibbens.

I don't see any questions coming forward, but I'd certainly encourage you to also provide a specific written submission with respect to sections of the act that you feel need to be stiffened up. We have until next Friday to do that.

W. Gibbens: I understand that February 29 is the...

R. Cantelon (Chair): Right.

W. Gibbens: I'll endeavour to prepare something.

R. Cantelon (Chair): Thanks for taking the time to come today.

We have no one else who's scheduled — actually, one who is scheduled has not appeared — and no others have come forward.

We'll take a ten-minute recess and give some time for members of the public or whoever wishes to come forward, and then we'll reconvene and consider whether to proceed or not at that time. We'll recess until 11:40.

The committee recessed from 11:33 a.m. to 11:50 a.m.

[R. Cantelon in the chair.]

R. Cantelon (Chair): I'd like to call the committee back to order. I see, in checking with the Clerk, that we have no further witnesses. Thank you for your participation, committee.

A motion to adjourn is in order.

The committee adjourned at 11:51 a.m.

HANSARD SERVICES

Director
Jo-Anne Kern

Manager of Print Production
Robert Sutherland

Post-Production Team Leader
Christine Fedoruk

Editorial Team Leaders
Laurel Bernard, Janet Brazier, Robyn Swanson

Senior Editor — Galleys
Heather Bright

Technical Operations Officers
Pamela Holmes, Emily Jacques, Dan Kerr

Indexers
Shannon Ash, Laura Kotler, Julie McClung, Robin Rohmoser

Researchers
Mike Beninger, Caitlin Roberts, Pavlina Vagnerova

Editors
Anton Baer, Catherine Cardiff, Aaron Ellingsen, Deirdre Gotto, Margaret Gracie,
Jane Grainger, Betsy Gray, Linda Guy, Barb Horricks, Bill Hrick, Paula Lee,
Nicole Lindsay, Donna McCloskey, Anne Maclean, Cristy McLennan,
Constance Maskery, Jill Milkert, Lind Miller, Lou Mitchell, Karol Morris,
Dorothy Pearson, Erik Pedersen, Peggy Pedersen, Janet Pink, Melanie Platz,
Heather Warren, Arlene Wells, Tara Wells, Glenn Wigmore

Published by British Columbia Hansard Services and printed under the authority of the Speaker.

www.leg.bc.ca/cmt

Hansard Services publishes transcripts both in print and on the Internet.
Chamber debates are broadcast on television and webcast on the Internet.
Question Period podcasts are available on the Internet.