



Third Session, 38th Parliament

REPORT OF PROCEEDINGS
(HANSARD)

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

Victoria

Tuesday, May 29, 2007

Issue No. 3

RON CANTELON, MLA, CHAIR

ISSN 1913-4746

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

Victoria
Tuesday, May 29, 2007

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)
Simon Gray-Schlehauf (Committee Researcher)

Witnesses: Mary Carlson (Office of the Information and Privacy Commissioner)
David Loukidelis (Information and Privacy Commissioner)
Errol Nadeau (Office of the Information and Privacy Commissioner)
Blair Stewart (Office of the Information and Privacy Commissioner,
New Zealand)

CONTENTS

Special Committee to Review the
Personal Information Protection Act

Tuesday, May 29, 2007

	Page
Briefing: Office of the Information and Privacy Commissioner	11
D. Loukidelis	
E. Nadeau	
M. Carlson	
Committee Meeting Schedule	19

MINUTES

SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT



Tuesday, May 29, 2007
8 a.m.

Douglas Fir Committee Room
Parliament Buildings, Victoria

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

1. The Chair called the Committee to order at 8:02 a.m.
2. The following witnesses appeared before the Committee and answered questions:
 - David Loukidelis, Information and Privacy Commissioner
 - Mary Carlson, Director, Office of the Information and Privacy Commissioner
 - Errol Nadeau, Manager, Investigations and Mediation, Office of the Information and Privacy Commissioner
 - Blair Stewart, Assistant Privacy Commissioner, New Zealand
3. The Committee discussed the plan to develop a preliminary business plan.
4. The Committee adjourned to the call of the Chair at 8:59 a.m.

Ron Cantelon, MLA
Chair

Kate Ryan-Lloyd
Clerk Assistant and
Committee Clerk

TUESDAY, MAY 29, 2007

The committee met at 8:02 a.m.

[R. Cantelon in the chair.]

R. Cantelon (Chair): Welcome, everybody. Good morning. We're not quite at full complement, but we're certainly at full quorum. The time has approached. We all have other things to do in our eagerness to fulfil our legislative responsibilities.

Mr. Loukidelis, the floor is yours, sir.

**Briefing: Office of the
Information and Privacy Commissioner**

D. Loukidelis: Thank you, Mr. Cantelon and Members.

I'd like to begin this morning by making some introductions to the committee. I have to my left here Mr. Blair Stewart, the assistant Privacy Commissioner for New Zealand, who is on his way back to New Zealand from some time in Ottawa with our federal colleagues and has been with us this week, working with us to introduce us to the way privacy is done in New Zealand. I'm very happy that he's been able to join us today. I'm sure he'll be able to answer all of the questions that I can't answer or that my colleagues can't answer.

To my right I have Mary Carlson, who is the executive director of my office, and Errol Nadeau, who is manager of investigations and mediation, responsible for the Personal Information Protection Act complaints and investigations. He manages our team of investigators as they do their work under this legislation.

I wanted to bring them and introduce them to you today because, together with me, they are available to the committee to help you in your work. Should you have need of any assistance, we're all available to do whatever we can to help the committee with its work.

My goal today is a modest one. I don't propose to repeat or cover the same ground as was covered by Sharon Plater for the Ministry of Labour and Citizens' Services when she appeared before you on May 16. I think it's quite evident that Ms. Plater covered a lot of ground. I think she did an admirable job of giving you a very good sense of what this legislation is about, the context for its enactment, both international and domestic, and some of the issues that have arisen, certainly from the government's perspective, in the first years of the life of this legislation.

What I propose to do today is say a few words about why the Personal Information Protection Act was and is a good policy choice for British Columbia. Second, I will give you an overview of the role of my office under the legislation and also outline in general terms how it is that we go about our work in providing oversight for compliance with the legislation.

Third, in a rather anecdotal fashion and using some statistics, I hope to describe some of our experience under the legislation to date in actually assisting organizations and their customers on the ground in complying with the legislation and with ensuring that

the rights of customers are respected. Last, I'll address a couple of specific points, including a couple of points that arise in light of Sharon Plater's appearance before you, about the legislation as the committee moves forward with its work.

[0805]

As a first preliminary point, though, I would like to, if I might, state here my recommendation for the committee's consideration: that the committee hold public hearings in the province and actively reach out to stakeholders. I say this because we have, over the last number of years, been quite active in dealing with a variety of stakeholder groups and individual organizations and their customers.

I know that there is interest out there in this legislation. It is legislation that has just been in force for roughly over three years. I think you'll find that there will be a number of groups, umbrella organizations and, in fact, individual businesses and other organizations that will be able to bring valuable perspectives, if I might suggest, to the committee's work.

Moving to the first area of my remarks, I just wanted to touch briefly on our perspective on why PIPA is a good policy choice for British Columbians.

R. Cantelon (Chair): I wonder if I could just hold you there. I forgot to introduce our panel, Mr. Loukidelis. I'd ask us, starting with Mary, to introduce ourselves.

M. Polak: Mary Polak, from Langley.

J. Rustad: John Rustad, from Prince George-Omineca.

L. Krog: Leonard Krog, Nanaimo.

R. Cantelon (Chair): I timed that to try and catch them with their mouths full of buns and so forth, Mr. Loukidelis. Excuse me for interrupting. Please continue.

D. Loukidelis: Thank you, Chair. That break allowed me finish my coffee as well, so I'm grateful to the Chair.

Our office supported the 1999 all-party recommendation for private sector privacy legislation in British Columbia, to which Sharon Plater referred in her appearance before you. We continue to believe that this legislation, in some sense, has levelled the privacy playing field for all businesses and organizations in British Columbia.

Like other private sector privacy laws, the Personal Information Protection Act enables businesses to realize the privacy payoff that flows from their implementing the recognition that good privacy is good for business. Customers and employees alike of organizations who are confident that the organizations with which they deal or that employ them will properly handle their personal information will be more likely to trust those organizations and to favour them either with repeat business or ongoing loyalty as employees.

I think this is an important feature of the legislation and one that our experience under the legislation to date indicates is very much a live feature of the legislation.

There is a recognition — a growing recognition, in fact — amongst the private sector organizations in British Columbia that good privacy is good for business and that this legislation helps them achieve that.

As regards to the legislation itself, of course, it deals with rights and interests of individuals and the organizations they deal with. It's an explicit goal of the legislation to find the balance, if you will, between the rights of individuals to a measure of protection for their personal information and also the interests of businesses and other private sector organizations in collecting, using and disclosing personal information in the course of their business or other activities.

We continue to believe that this legislation strikes, overall, the appropriate balance in terms of providing a set of commonsense rules that give businesses, and customers in particular, considerable latitude to make their own choices and bargains while at the same time ensuring that there is appropriate protection for personal privacy.

One preliminary point that I wanted to make at this stage, just almost as an aside, is to bring to the committee's attention the fact that although Quebec, Alberta, British Columbia and the federal jurisdiction are the only jurisdictions in Canada that have what you might call plenary private sector privacy legislation, it is important to point out that the private sector's practices in the collection, use and disclosure of personal information are, in fact, regulated elsewhere in Canada through so-called health privacy laws.

Ontario, most recently under the Personal Health Information Protection Act, regulates the practices of the private sector when it comes to the collection, use and disclosure of personal health information. Similar laws exist in Manitoba, Saskatchewan and Alberta. Alberta has three privacy laws — one affecting the public sector and two affecting the private sector. It's important to underscore at this point that we do have private sector privacy legislation that is sector-specific but that exists in jurisdictions other than the ones I've mentioned or that have been mentioned to you previously.

[0810]

There is a considerable record of experience out there, legislatively and operationally, on the ground with health privacy laws. This may be of assistance to the committee as you go about your work in examining how the legislation here in British Columbia affects certain sectors of the economy, specifically the private health sector, which of course plays an important role in delivering health services to British Columbians.

The second area that I wanted to touch on is the overview of our role in providing oversight of compliance with the Personal Information Protection Act. Our main function under that legislation is to provide that oversight and enforcement. We also have, however — and I think it should be mentioned at the outset — the mandate to provide public education and to engage in research on any matters that affect compliance with the legislation.

We have power to comment on the privacy implications of proposed programs of specific businesses or other organizations. We have the authority to comment on the implications for privacy of record linkages — so-called data matching. We also have the authority to comment on the implications for privacy of automated information systems. A variety of proactive powers are available to us in assisting the private sector in complying with this legislation.

It has to be said, however, that apart from our public education role — and I'll have something more to say about that in a moment — our main activities under this legislation since it came into force at the beginning of 2004 have been in the oversight area — in handling of complaints, conducting investigations, mediating settlement of disputes and more rarely, quite candidly, issuing binding orders to ensure compliance with the legislation.

We don't emphasize the order-making power. In fact, as we have always done under the public sector privacy and access-to-information legislation, we emphasize resolution of disputes wherever possible through mediation.

Our general approach when a complaint is made to us is to refer it to mediation by one of our portfolio officers, who will inquire into the facts surrounding the complaint and will, wherever possible, attempt to settle the matter with the agreement, obviously, of both parties in a way that both ensures vindication of the legislatively protected privacy rights of the individual involved and provides a commonsense, legally compliant, forward-looking resolution of the business practice in question so that the business is in effect encouraged, through the recommendations resulting from the mediation, to improve its practices and to come into compliance with PIPA.

I have thought that this was especially important in the early days of this legislation, which undoubtedly, it has to be said, I think represented for many organizations in the private sector a change in the way they do business. We are still in that position. We still emphasize mediation, education and support wherever possible in trying to assist organizations to come into compliance with PIPA and to ensure that their privacy practices are indeed best practices.

We will, from time to time, having investigated a complaint in the manner I've described, issue investigation reports, which are publicly issued. They contain recommendations for action on the part of organizations but generally speaking go no further than that. They are not binding in the sense that they're technically a use of the order-making power that is given under the Personal Information Protection Act.

They try to encourage compliance but also to encourage compliance more broadly by bringing to the attention of the public — including, of course, other organizations and their customers — what happened in the particular case, what our findings of fact were and what our recommendations were for improvement, so that other organizations can benefit from the work that we've done.

I might also add and should have mentioned a moment ago that even with the mediation activities — even with settlement of disputes through mediation by a portfolio officer — we do publish on our website anonymized summaries of the outcomes of mediation, and that of course is part of the public education role. We're trying to bring to the attention of organizations the outcome of specific disputes. We've provided you, in the material that was distributed before today's meeting, examples of some of those mediation summaries in the brief that you'll find at tab 1 of the materials that were delivered to you.

[0815]

Generally speaking, I think it should be underscored here that we have worked with a policy of referral. I have the authority under the Personal Information Protection Act to refer would-be complainants back to the organizations involved, including where there are other perhaps more appropriate oversight systems available or where, for example, there might be another method of resolving the particular dispute.

I think it's appropriate at this time to be reviewing our policy on this, not with a view to no longer doing it but with a view to ensuring that the policy remains current, given our present experience under PIPA, and that we're referring things back to organizations appropriately. Of course, when we do this, we're saying to would-be complainants: "We want you to try and resolve this first with the organization you're dealing with. If you're an unhappy customer of a particular business, we would prefer that you try and work this out with the business and come to some resolution."

What we're finding is that quite a number of the complaints that we would otherwise have to deal with are being resolved in that fashion. There may have been a misunderstanding — a lack of clarity in terms of the customer's expectations, a lack of understanding on the part of the organization about its PIPA responsibilities. When we refer these people back, we do provide both the would-be complainant and the organization with supportive information about PIPA and what it entails. We do follow up — not in every case, perhaps, but as many as we can — to ensure that the dispute was properly resolved.

Certainly, in the early days of PIPA, again, I continue to believe that this is an appropriate approach wherever possible. There are cases where we don't require people to go back — because there might be further victimization of an individual in an employment setting, for example. I do think, though, that generally speaking, this policy of refer-back assists organizations as well as their customers and employees in coming into compliance and continuing to comply with the legislation.

The last point in terms of the overview of our formal activities under the legislation is the order-making power. As I indicated a few moments ago, there have been relatively few of those orders in the three years since PIPA came into force. I'll mention only two of them just to illustrate how it is that they can play an important role in ensuring the legislation is meaningful on the ground.

The first order that I issued, after a formal inquiry with submissions and evidence, involved a retail organization that had been collecting identifying information of customers who wanted to return goods for refund or credit. Because of concerns around fraud, they were collecting the identifying information and keeping it on file so that they could ensure, essentially, that people weren't engaging in fraudulent activity by returning goods all of the time.

At the end of the day, I upheld the practices of that organization, although I held that they could not use that same information for customer satisfaction follow-up surveys. The stated purpose was for fraud prevention, and I held them to that. I didn't allow them to use it for that collateral purpose, for which they had not obtained consent, having given notice, as required by the act.

Similarly, I also ordered them to devise a retention period for the retention of that personal information. Their position had been that they should be entitled to retain this information indefinitely, and I required them to go back and devise a retention period and bring it back to me, which they did, ultimately, and which I found was acceptable.

Another order that might be of interest had to do with a film company based in the United States that was filming productions in Vancouver and was requiring film crew members to provide information to prove residence so that the corporation could qualify for provincial and federal film and video tax credits. An individual complained to us and said that this requirement as a precondition of employment was an unreasonable act and indeed infringed on that person's privacy.

At the end of the day, I found that the organization was entitled to do this under the special employment privacy provisions of PIPA, under the employee personal information provisions, and I held that this was a reasonable practice because they were being duly diligent in order to be able to prove to the government agencies involved that they were entitled to these credits.

The last point I will make is that we do devote a considerable amount of our resources to education of organizations and individuals in a variety of ways. As our resources permit, we are active in proactively providing support materials for organizations and for the public. Rather than taking you through each one of them, I'll just refer you to the materials that have been provided to you at tab 3 of your material.

You've been provided with a list of the resources that we provide for private sector organizations and members of the public, some of which are a general overview, for example, of the legislation in our guide for businesses and organizations. That's at tab 2 of your material. But also, more specific materials deal with issues, for example, around the security of personal information when individuals are working away from the office, in essence preventing personal information from being stolen while out of the office; special guidance on social insurance numbers; key steps in responding to privacy breaches; and so on.

[0820]

On the other side of the equation, if you can put it that way, are resources for members of the public to inform them about their privacy rights under the Personal Information Protection Act and how they vindicate those rights, including through making complaints to our office.

The third area that I wanted to cover has to do with our experience under PIPA to date. As I mentioned, I propose to do this in a largely anecdotal fashion. Starting with some figures for you, our preliminary figures for the fiscal year ending March 31, 2007, indicate that during that fiscal year we opened 103 formal complaint files, bearing in mind again this policy of refer-back that I described a moment ago. During that fiscal year we opened 59 files that we term requests for review, where individuals have, for example, sought their own personal information in the hands of an organization and haven't been satisfied with the response.

In '06-07 there were 103 complaint files opened formally and 59 requests for review. Again, these are preliminary figures. I have the numbers here for the files that we closed in 2005-2006. We closed 146 complaint files and 49 request-for-review files. In the year before that, in 2004-2005, which obviously would have included the first year of PIPA's existence, we closed 53 request-for-review files and 118 formal complaint files.

As the mediation summaries that I've provided in the briefing document illustrate, there is a wide variety of situations generating the complaints that arise. Our early impression under PIPA was that the majority of inquiries — that is, for information from our office and formal complaints under the legislation — would involve smaller organizations, and that has been borne out. British Columbia has a relatively high proportion of small and medium-size enterprises in our economy, and our experience to date indicates that it is the smaller organizations that have been a large part of our business.

Early on we received more complaints against retail stores and insurance and financial institutions than we seem to get these days. Generally speaking, these organizations or their umbrella trade organizations had the resources to develop and refine their privacy policies and dispute resolution mechanisms. The Retail Council of Canada, chamber of commerce and, in the case of credit unions, the Credit Union Central have been active in helping their members as time has gone on come into compliance with PIPA. So over time we've seen the proportion of complaints coming from those sectors decreasing somewhat.

The largest volume of complaints and requests for review that we now receive are generated by employees of small businesses concerned about their employers' information practices or, more commonly, former employees seeking their own personal information after their employment has terminated. Again, we're trying to work proactively in this area by providing support tools for businesses and indeed employees and former employees. You'll see listed at tab 3, "Frequently asked questions," for example, on collection, use and disclosure of employee personal information: "Attempting to respond

to and in some senses anticipate the need for guidance from our office on employment-related privacy issues."

Another area that has seen a lot of activity is in respect to housing, including issues involving strata corporations, housing cooperatives and residential tenancies. These generate the next-highest volume of inquiries and complaints to our office. This may of course be due to the nature of the housing market at present, but certainly we do get a considerable number of requests for information and some complaints in this area. We're in the course of developing resource materials to assist landlords and tenants and strata corporations to ensure that the obligations under the legislation are met.

There was a story over the weekend, for example, in the *Globe and Mail* about a new service available to landlords in the lower mainland, at least, of the province in performing criminal-records checks, credit checks and background checks on would-be tenants, and the maintenance of a bad-tenant database. Having had that brought to my attention over the weekend, on Monday we contacted that organization and offered our assistance in ensuring that the extensive collection and disclosure of personal information that appears to be occurring does comply with PIPA and good privacy practices.

[0825]

The last sector that has generated activity that I think merits mention today is in the area of professionals — whether it be legal professionals, health care professionals or others — who are of course operating essentially as small businesses. These have generated a relatively significant proportion of our requests for information and complaints, most often in the area of access requests. This is where individuals seek access to their own personal information, particularly in relation to fees assessed by these organizations for providing individuals with access to their personal information.

These complaints have decreased somewhat in number as PIPA has matured, but certainly, early on we did experience and continue to experience to some degree activity in this area. We have worked with, for example, the Law Society of British Columbia, the College of Physicians and Surgeons and the B.C. Medical Association in helping them help their members ensure that they stay on side with PIPA in, for example, the area of providing access to information and in the charging of fees.

The last area that I would like to touch on is really just to address some of the points that were mentioned in Sharon Plater's appearance but also a couple of specific points that might be of interest to the committee today, bearing in mind that you're relatively early in your work and that other issues may well arise.

One of the areas that I think you are likely to be hearing us speak about more and more in the coming year or so has to do with so-called privacy breaches. These have been much in the media lately. The question of identity theft.... Not only public concern about identity theft but the hard numbers that indicate that identity theft is, if you will, a growing business sector for those engaged in that illegal activity have meant that we

have tried as proactively as possible to deal with some of the issues around privacy breaches, which of course entail the unauthorized disclosure, generally speaking, of personal information.

We had 34 reported privacy breaches in both sectors last year, and 12 of those were in the public sector. We have done a number of investigations in order to ensure that organizations comply with their legal obligation under this legislation to take reasonable measures to protect personal information against unauthorized use or disclosure.

We've also, though, more proactively.... With our colleagues in Ontario in the Information and Privacy Commissioner's office there, under their private sector mandate to do with health privacy, and more recently with our federal colleagues, we have worked to publish a number of documents that help organizations realize, if you will, their obligations.

We have published, for example, key steps in responding to privacy breaches. We have given them a brief breach notification assessment tool. It allows them to decide on a risk assessment approach, whether it's appropriate or indeed necessary to notify customers or patients or clients that their personal information has been lost, so that those individuals can take steps to protect themselves, particularly against identity theft.

Turning to the health sector more specifically, we have worked with the BCMA and the college to publish *Key Steps for Physicians in Responding to Privacy Breaches*. I wanted to emphasize this area because I think it really illustrates in an important way, to my mind, how the Personal Information Protection Act has changed the landscape for private sector organizations in the province.

Until that legislation came into force, there was certainly no statutory and perhaps no other legal obligation on organizations to take care to protect customer information. There is now a positive, explicit duty for them to take care to protect customer or client information. I think that it illustrates how PIPA changes the landscape, as I say, by imposing, quite frankly, an important privacy protective measure on the private sector. But with the clarity of that legislated obligation, it also gives them an opportunity, as may be illustrated by our work, to show their customers and clients that they're taking their privacy responsibility seriously.

Customers, clients and patients expect organizations to deal with their personal information in a responsible manner, quite apart from what the legislation says. I think that this illustrates well that PIPA underpins the reasonable expectations of the public and assists private sector organizations in understanding that there is an advantage to having good privacy practices that will meet those expectations in the economy.

Looking forward. Our submission, when we do make one to this committee at the appropriate time, will, I expect.... My present intention — let me rephrase that — is that we will almost certainly be addressing our enforcement powers — how the legislation is crafted in terms of the role that our office formally plays in investigating and attempting to resolve concerns around

privacy practices. I think it's fair to say that the drafting of the legislation is perhaps not as elegant as it could be in that respect.

[0830]

There are a number of methods of getting in the door on a formal basis with our office in terms of making a request for review or laying a complaint. There are different legislative provisions or nuances in those provisions in terms of how we have to respond and what our powers are to move forward.

I'm very, very likely to come to this committee and recommend changes, similar to those that are now before the House in the form of Bill 25, in relation to the Freedom of Information and Protection of Privacy Act and our powers under that legislation, in part to ensure that when we do our work under either this legislation or the public sector legislation, our powers are similar, because it makes for efficiency, clarity and certainty, but also to address what I think are some of the issues in the drafting of the Personal Information Protection Act.

We may well have other suggestions for you in terms of the drafting of that legislation, because there are certain respects in which, with deference, I think it could improve in terms of its clarity and its certainty for those who actually have to comply with the legislation as well. It's not just an issue of our work and how we go about our work.

The last point I'll make is that I think, generally speaking, the legislation works well. It provides, I believe, a balanced set of rules that accommodate well the needs of the public and also of the organizations affected by this legislation. Although the committee may well find areas for improvement — and I've touched on a couple of those from our perspective — I think the legislation has so far stood the test of time well and is something that British Columbians should be proud of.

R. Cantelon (Chair): Thank you.

Our Deputy Chair has joined us. I'd ask the member for Yale-Lillooet to introduce himself to the panel.

H. Lali (Deputy Chair): Hi. Harry Lali, MLA for Yale-Lillooet.

R. Cantelon (Chair): Now, are there any questions or issues that any of our panel, our commission, wishes to raise?

L. Krog: Staff time. Appreciating that your office has many functions and responsibilities, can you give me some idea of the percentage of staff time that's spent with respect to PIPA?

D. Loukidelis: I'll ask my colleagues to express their views as well. I think we do not track that with precision. We don't keep time in that sense. My sense of it, though, is that the bulk of our work remains in the public sector — the oversight role under freedom of

information but also public sector privacy. And I think it's fair to say that it's an increasing proportion. I would say that this legislation probably engages our attention about 15 percent of the time.

Again, I'm quite happy to hear what my colleagues have to say. Errol Nadeau is much more directly involved, as is Mary Carlson in many respects.

E. Nadeau: The pool of portfolio officers who mediate and investigate complaints do that under both the Freedom of Information and Protection of Privacy Act and the Personal Information Protection Act, so there's some overlap there. We have a manager of investigations and mediation to assist that group of employees for the public sector legislation and another for the private sector legislation.

Our intake function, where complainants have their first contact with the office, spends a considerable amount of its time providing information about the legislation. Their statistics show that almost half their time is spent in responding to inquiries about the legislation. Again, our efforts with respect to providing materials and guidance for the public and for organizations are a fairly considerable amount of our time.

In terms of complaint and mediation, the proportion of the work under the public sector legislation is considerably greater, but in the other areas I would say it's roughly equal.

M. Carlson: I would just like to add that 162 private sector privacy files last year would represent a full caseload for two of the investigators. On the public side, most of our work is requests for review. They're access requests, and those are actually easier to resolve.

[0835]

The trickier ones are privacy complaints. Most of the files we deal with in the private sector are privacy complaints. They're more time-consuming because we're going in to investigate an organization that may never have heard of us before. When we investigate the public sector, they know who we are. They're not happy to see us most of the time, but they know who we are, and they know what the rules of engagement are.

There is considerably more effort that has to go into investigating private sector privacy complaints. We have to tread more softly and spend more time up front doing some education about who we are and what the expectations are.

L. Krog: I'll raise a very basic example that strikes me. Consumer purchases now — it's obvious that they track your purchasing. All sorts of stores offer cards and discounts and whatnot, so that for everything you purchase, that information is in theory available — what kind of toothpaste you use, whether you buy muffins once a week or once every second week. I'm raising this around the issue of identity theft and things of that nature, as well, and how that information is traded.

Does your office independently investigate that? Does it track it? For instance, Save-On-Foods....

Interjection.

L. Krog: One of my colleagues indicates she likes Save-On. I'm sure she does. It's a good union operation. I'm delighted she supports it.

Nevertheless, this growing compilation of information about everything we do and everything we purchase, how many Starbucks we buy and all of that.... Does your office do any independent investigations just on its own initiative? Does it even have that authority under the act to ensure that there is compliance?

D. Loukidelis: There is authority under the act for me to initiate on my own motion a so-called commissioner-initiated investigation, where I have essentially reasonable grounds, to paraphrase, to believe that a breach of the act might have occurred. We are almost exclusively reactive, candidly, in terms of investigating complaints that are brought to us. So although we have the commissioner-initiated investigations — the audit capabilities to which I referred earlier — we do focus on responding to complaints.

The particular example you've given is a good one. It raises pretty broad privacy issues. Of course, under both our legislation and the federal private sector privacy legislation, to give another example — and Alberta, for that matter — that kind of collection, use and disclosure of information — the compilation of purchasing habits and so on about individuals — can only proceed with notice and consent. If you read the fine print when you sign up for the loyalty card, you'll find that you're essentially consenting to all of that being done.

I think one of the interesting things about this, however, is that individual consumers who sign up for these cards may not appreciate the extent or breadth of the collection and disclosure of that information and the power that it really carries with it. That's not to say that I think it's improper or shouldn't be permitted, but I do think that education of consumers is something that should be considered, and they should be aware of what it is they're getting into.

I can assure you that I've been assured by a marketing executive that data-mining techniques applied to databases of this kind can, with a high degree of confidence, statistically speaking, correlate between consumption of a particular breakfast product and mortgage default.

L. Krog: Which — if I, with the indulgence of the Chair, may continue — leads me...

R. Cantelon (Chair): One more, and then we have a couple of others.

L. Krog: ...to the issue of informed consent. My guess — it's one of the reasons I raise it, and you've hit it on the head — is that I don't think the average consumer signing up for any of these understands what it means in terms of being able to create a portrait of them as a family or an individual.

I'm just wondering if there's any legislative change required or if you have any comment or recommendation around that. My concern, frankly, is that an 18-year-old high school student standing at a Future Shop store or at the desk at Save-On or whatever is not going to provide some informative explanation of what it is you're giving away when you sign up.

[0840]

D. Loukidelis: I think that under the existing legislation, the requirements for adequate or appropriate notice should be able to deal with that. Having said that, is there room for more education not only of organizations but of consumers before they sign up for these things? Yes, I think there is. It's always a difficult thing to try and educate individual consumers in terms of reaching them.

Another illustrative anecdote is that last Easter at a single London Underground station, two people stood outside with a clipboard and, with a promise of £80 worth of chocolate, within 20 minutes collected something like 68 individuals' personal information sufficient to steal their identities. These individuals didn't identify themselves. They had a clipboard with what appeared to be a questionnaire. In exchange for this vague promise of £80 of chocolate, 68 people gave up all of their personal information that would be necessary for identity theft purposes.

J. Rustad: That's an interesting example — the one you've last given.

I just wanted to make a little comment. The member always likes to bring up Starbucks, which is a great example of capitalism. I'm pleased to see him supporting that kind of concept.

L. Krog: You assume too much.

J. Rustad: Sorry. I digress.

Reading through it, the Personal Information Protection Act is really about information, whatever form it happens to come in. I have some concerns or some questions around the use of technology and the fact that when you fill out a form at a particular store or doctor's office or wherever it is that you may fill out a form, that usually stays within that organization or within that office. When you do something on line, that could very easily go immediately to the Cayman Islands or United States or Russia or wherever, which may not, obviously, fall within the rules and regulations that we have here.

I guess the question is: in terms of the act, is there anything that we need to be looking at around technology, around the globalization of information through the utilization of technology? Is it just buyer beware or wild, wild west, or is there anything meaningful that can be done?

D. Loukidelis: Two points in response to that very good question. When it comes to rapidly evolving information technologies and the commensurately rapidly

evolving risks to personal information security because of hacking and other illegal use of those technologies to create threats for personal information security, this legislation, like other legislation in Canada, is technologically neutral. It imposes an obligation on private sector organizations to take reasonable measures to protect personal information from unauthorized collection, use, disclosure, retention or destruction.

I, certainly for my part, continue to support that technologically neutral approach. It is an obligation to take reasonable measures. It can evolve as technologies and threats evolve as well. Looked at from the private organizations perspective, it's a question of simply ensuring that your information security measures keep current with the threats. I would not at this time suggest to the committee a technologically prescriptive approach to information security. It is always a game of catch-up, and it can have consequences for organizations.

We haven't seen it yet here in British Columbia, but to bring in a question that was asked in an earlier meeting of the committee, it is possible for individuals to sue for damages under this legislation. If someone comes to us with a complaint and I make a finding that the organization has not appropriately protected personal information that was lost and that individual has suffered actual harm — it's actual harm that is the touchstone of liability here — that affected individual can go to the Supreme Court of British Columbia and get damages as compensation.

With the class action proceedings legislation we have here in the province, there may well be cases arising that allow that obligation to bite quite hard, actually. We're seeing examples elsewhere in Canada. There have been class actions brought already. I think that will bring home to organizations the need to ensure that they take the appropriate measures to protect personal information when it comes to information systems.

[0845]

The second point is touching on the globalization of data flows. They've been called the new spice routes. The flows of personal data in the ordinary course of commerce are ever wider and moving more quickly. Information flits around the globe daily.

This legislation — and it's the same in other jurisdictions in Canada — does not restrict export of personal information and does not take an approach similar to that found in some European countries, for example. The challenge is to try and achieve, I think, a globalized privacy standard or framework that can encourage all economies engaged in trade to adopt legislative protections or other kinds of protections for privacy that as far as possible approach what we have here in British Columbia.

My colleague from New Zealand, Blair Stewart, who is here today, has been very active in the Asia-Pacific Economic Cooperation organization's efforts to standardize privacy protection around the globe. I, certainly for my part, would be encouraged if that continued to be the approach taken here in Canada. I would not be in favour of any amendments to our own

legislation that would import data export controls into the legislative framework.

An organization here in British Columbia that's going to export personal information of a customer outside of British Columbia's borders, in my view, remains bound by this legislation. So it's up to them, by contractual measures or otherwise, to ensure that they stay on side with this legislation.

By contracting out — for example, with a service provider elsewhere in the Asia-Pacific region or in Ontario for that matter — in my view, they're not then going to absolve themselves of responsibility under this legislation. They had better take the steps they need to take to ensure that they stay on side with the legislation, because they will remain accountable for what happens to the information outside of British Columbia.

J. Rustad: Can I do a follow-up? You touched on something that I found quite interesting, and that is the idea of standardizing PIPA and PIPA-like legislation around the globe and the efforts that are going on. Would it be worthwhile for us to look at the work that is ongoing and see where our legislation fits in roughly with the work that's been done to date in terms of standardization?

D. Loukidelis: It may be of use to the committee as a contextual exercise to have regard to what's being done elsewhere. The APEC privacy framework, which was adopted by the APEC leaders in November 2004, including Canada, is a framework that is readily met by PIPA. PIPA certainly meets the standard set out in that framework.

There are nine principles — fair information practices, as they've been called. PIPA is fully compliant with that and indeed takes — and Canada is known for this around the Asia-Pacific region and the globe — a balanced approach to these things, which is seen not to excessively regulate and not be too directorial but at the same time provides meaningful protections. It is a legislative, regulatory approach as opposed to a self-regulatory approach, and it contains meaningful protections for personal privacy, in my view.

M. Polak: You mentioned that other provinces have separate legislation governing the collection of health information. How is British Columbia situated, given that we're obviously seeing some shifting in terms of private organizations' involvement in health care? How are we situated with respect to that?

D. Loukidelis: The situation in British Columbia, given the extent of private sector involvement in the delivery of health care — whether it be physicians, medical laboratories, pharmacists, pharmacies and so on — is divided. On the public sector side, of course, we've always covered the health sector in British Columbia, which is not the case in Ontario. Hospitals and health authorities were not covered under their legislation.

Under the Freedom of Information and Protection of Privacy Act, the public sector is not subject to a consent obligation. Public sector organizations need only have statutory authority or a need for personal information that they want to collect to deliver a program or a service. PIPA, which applies to the private sector participants in the health system, of course has a consent standard, by and large, with some exceptions — for collection, for use and for disclosure, of course.

The approach that PIPA takes, though, I think, is such that it can work and in my view does work well in relation to health services. The question that remains, given that there is this divide across which there are health services delivered, is whether health privacy legislation is needed in the province.

[0850]

In Alberta you have three pieces of legislation that apply in any given moment, perhaps. Obviously, it's a question for legislators whether we need a third privacy law here in British Columbia that applies across that divide and that is sector-specific.

Quite candidly, that's the approach that has been taken now in four provinces, four jurisdictions, in Canada. It's not something that, speaking personally, we would necessarily leap at seeing in the province, but it is something that may well bear consideration.

R. Cantelon (Chair): I have a couple of questions. One relates to the general field of identity theft. I'd like your comments on whether you see that as a growing issue.

A specific question — and you can begin with this one — raised by a constituent was that the last four digits on a credit card, I understand, are the ones that give personal identification. It has been recommended that we legislate or otherwise regulate the distribution of those last four numbers.

Some credit granters, as you know, X them out or don't print them, but smaller businesses do print them, and then, of course, the receipts are around. Could you comment on that and more broadly on what seems to be a rising concern in the public, as I've heard, over identity theft?

D. Loukidelis: Taking the second issue about the credit card numbers, until quite recently many point-of-sale terminals were printing the entire credit card number with expiry date and name. I was told by commercial crime police officers in Vancouver about two years ago that a credit card receipt with all of that information was worth \$15 to \$20 on the street because, of course, it gave you what you needed in order to commit credit card fraud.

We've seen a move as, especially, smaller businesses find it possible for them to pay for the new technology, and the large organizations — the bank-run or financial institution-run organizations that operate these point-of-sale systems — have moved towards the situation you've described. I don't know, quite frankly, whether technically that's adequate security, but it's sure a lot

better than printing more of the numbers. Most of them do just print the last four digits. They don't even show the issuing institution, which is the first four digits of a credit card number.

Whether that's too much information is something that the experts would have to answer. I can tell you that we've been pleased to see only those last four digits printed. They are the personal identifiers, but without the rest of the information, you don't really know what the credit card is. That's my understanding, but again, I'd defer to the experts on that.

Identity theft, as I indicated earlier, is growing. I don't have statistics at my fingertips, but in Fraud Awareness Month every March you see new numbers coming out of the law enforcement agencies in this country that indicate it is a growing problem. It is a big concern for individuals, even if in most instances — credit card fraud, for example — it's actually the financial institutions that directly bear the cost, which of course they then pass on to all of us.

There are a number of solutions. Again, I think that using this legislation as best we can to bring home to organizations their responsibilities to protect customer information.... Criminalization of some of the associated activities is one avenue that we've supported. I know my federal colleague has, and parliament is looking at criminalizing certain acts that aren't now an offence.

It's an offence, obviously, to impersonate someone to commit fraud, but it's not an offence to possess personal information with intent to commit identity theft or to commit a criminal offence. This is something that parliament is looking at.

I think financial institutions and other private sector organizations have to continue to be part of the solution, as do customers in terms of how careful people are about their own personal information — throwing out credit card receipts or other sensitive financial information without ensuring that it's appropriately protected, just putting it into recycling, for example. There are steps that everybody can take, I think.

R. Cantelon (Chair): Okay. Do we have any other questions or issues anyone wishes to raise?

Hearing nothing further, I thank you and your guests and panel for a very informative morning. I'm sure this will be just the beginning. I'm sure that once we proceed, there will be a lot more questions and a lot more information that we'll require. Thank you for giving us this presentation today.

D. Loukidelis: Thank you for the opportunity. If we can be of any assistance at any time, you need only ask.

Committee Meeting Schedule

R. Cantelon (Chair): Moving on, I think that with the committee's indulgence, what I'm suggesting, to proceed, is that the Clerk will prepare an operation plan

— a business plan, essentially — which will involve lists of stakeholders and a potential schedule of meetings to have open hearings.

[0855]

We're not required to report out until next April, but I think that in terms of looking ahead to a time line, it's.... I'll try to avoid puns, but it seems to be a quiet issue in many respects. I don't think we should necessarily rush. Therefore, I would suggest that we look towards gathering information over the summer and the fall and then reporting out by the start of next parliament in February.

What I would suggest we do is prepare this plan, and with the concurrence of the Deputy Chair, we'll circulate it. I'd just as soon not have us all back, but if you wish, we could come back to approve that agenda sometime in June. If everybody can make their comments by e-mail, with the Deputy Chair's concurrence, then we would lay out a schedule for meetings.

How does that sound to everybody? Comments?

L. Krog: I'm very cognizant of what the Information and Privacy Commissioner recommended this morning in terms of public hearings. I'm just wondering if the Chair or the Deputy Chair have given any thought to it or had discussions or if the Clerk has any recommendations around hearings and what we're contemplating. Would it be a Victoria-Vancouver kind of affair, or are we talking about perhaps doing something a little more inclusive of the people who live outside the Big Smoke?

R. Cantelon (Chair): The original committee met in Vancouver and Victoria. That was kind of my thought — that we would meet in Vancouver and Victoria sometime, probably in September. But I'd hear any further suggestions if you wish.

J. Rustad: Maybe we should go out to Prince George sometime.

H. Lali (Deputy Chair): There are a few small centres around the province I think we could probably get to. Prince George is one, Kamloops, maybe something up-Island.

M. Polak: Shall I pitch in and say Langley now? Is that what we're doing?

A Voice: Fort St. John would be great.

R. Cantelon (Chair): Why don't I suggest, then, that when we put the plan together, we'll have sort of option A, option B, perhaps option C. Then we can see if the net is broad enough. Does that sound agreeable? And we'll compare it to the original.

When the committee first met, I don't believe they had extensive attendance at these meetings, so I think we want to bear in mind that we don't want to go a long way to meet nobody there.

J. Rustad: That might be a point we might want to pursue — to perhaps even do a little bit of inquiry as to the level of interest in various areas. If there are some responses, if there's an indication of interest, we might want to consider it.

R. Cantelon (Chair): What we heard, from what I've learned, is that principally it'll be stakeholder groups that will come, with some individuals. But mainly we'll take direction from major stakeholder groups, which are certainly happy to meet in Vancouver and Victoria. We don't want to omit anybody, though.

M. Polak: It would stand to reason, though, that the organizations that you determine are the ones you want to meet with are going to determine location to a certain extent.

R. Cantelon (Chair): Exactly. If that's agreeable, then, what we'll do is get a business plan with a couple of options and circulate it to everybody. Then the Deputy Chair and I will consult and confer, and away we go.

Hearing no further business, a motion to adjourn.

The committee adjourned at 8:59 a.m.

HANSARD SERVICES

Director
Jo-Anne Kern

Manager of Print Production
Robert Sutherland

Post-Production Team Leader
Christine Fedoruk

Editorial Team Leaders
Janet Brazier, Robyn Swanson, Antoinette Warren

Senior Editor — Galleys
Heather Bright

Technical Operations Officers
Pamela Holmes, Emily Jacques, Dan Kerr

Indexers
Shannon Ash, Laura Kotler, Julie McClung

Researchers
Mike Beninger, Caitlin Roberts, Sarah Towle

Editors
Laurel Bernard, Catherine Cardiff, Andrew Costa, Aaron Ellingsen,
Heather Gleboff, Margaret Gracie, Jane Grainger, Iris Gray, Linda Guy,
Barb Horricks, Bill Hrick, Paula Lee, Elizabeth Levinson, Nicole Lindsay,
Donna McCloskey, Cristy McLennan, Marg MacQuarrie, Constance Maskery,
Jill Milkert, Lind Miller, Lou Mitchell, Karol Morris, Dorothy Pearson,
Erik Pedersen, Janet Pink, Melanie Platz, Robin Rohrmoser,
Heather Warren, Arlene Wells, Tara Wells

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.