



Third Session, 38th Parliament

REPORT OF PROCEEDINGS
(HANSARD)

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

Victoria

Wednesday, May 16, 2007

Issue No. 2

RON CANTELON, MLA, CHAIR

ISSN 1913-4746

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

Victoria
Wednesday, May 16, 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-Schleihauf (Committee Researcher)

Witnesses: Sharon Plater (Ministry of Labour and Citizens' Services)

CONTENTS

Special Committee to Review the
Personal Information Protection Act

Wednesday, May 16, 2007

	Page
Personal Information Protection Act Overview.....	3
S. Plater	

MINUTES

SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT



Wednesday, May 16, 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

Unavoidably Absent: John Rustad, MLA

1. The Chair called the Committee to order at 8:04 a.m.
2. The following witness appeared before the Committee and answered questions:

Sharon Plater, Director, Information Policy & Privacy Branch, Ministry of Labour and Citizens' Services
3. The Committee adjourned to the call of the Chair at 8:52 a.m.

Ron Cantelon, MLA
Chair

Kate Ryan-Lloyd
Clerk Assistant and
Committee Clerk

WEDNESDAY, MAY 16, 2007

The committee met at 8:04 a.m.

[R. Cantelon in the chair.]

R. Cantelon (Chair): Good morning, everybody. Welcome to the second official meeting of the Special Committee to Review the Personal Information Protection Act.

We'd like to welcome Sharon Plater today. Thank you for coming, Sharon.

I'd ask committee members, starting with Leonard, to introduce themselves.

L. Krog: Leonard Krog, MLA for Nanaimo. Good morning, Sharon.

J. Schofield: Josie Schofield. We've already met — about three years ago on another committee.

K. Ryan-Lloyd (Clerk Assistant and Committee Clerk): My name is Kate Ryan-Lloyd. I serve as Clerk to the committee.

R. Cantelon (Chair): Ron Cantelon from Nanaimo-Parksville. I'm the Chair.

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

R. Cantelon (Chair): And regrets from John Rustad, who's under the weather this morning. I think Mr. Lali, the member for Yale-Lillooet, will be joining us later.

With that, I'd like to give the floor over to you, Sharon. You can proceed to give us some background information on this.

Personal Information Protection Act Overview

S. Plater: Okay. My understanding this morning is that's what I'll be doing — giving you a bit of background information on the legislation and also helping you to understand what the legislation is all about. I have given you a PowerPoint presentation that follows along with what I'll be presenting.

[0805]

What I'm going to try to do this morning is give you an idea of what the Personal Information Protection Act is, which I will refer to as PIPA, just to make it nice and short; give you a bit of the historical backdrop; an overview of PIPA's principles; briefly mention the implementation tools, which you have in a package in front of you that you can take away and look at. I'll give you an idea or update on what the recommendations were from the special House committee that reviewed the Personal Information Protection and Electronic Documents Act — that was a federal committee — and then open it for questions.

What is PIPA? PIPA is protection for personal information held by the private sector, the non-government

sector. B.C. already has the Freedom of Information and Protection of Privacy Act for the government sector. This is for the private sector. It's a commonsense set of rules for the collection, use, disclosure, retention and security of personal information.

When we were talking to businesses, we always used to frame it as: if you think about how you would like to have your information handled, then you're probably on the right track. It recognizes the right of individuals to protect their personal information and the needs of organizations that collect, use and disclose personal information for reasonable purposes. We believe that it did strike the right balance between those two interests.

One of the things that you will find in the Personal Information Protection Act is that a lot of it is based on the reasonable person test. In its purpose statement it says that what you're looking at is: what would a reasonable person expect to have happen in these circumstances? You will see the word "reasonable" come up throughout the legislation.

It was a response to the Personal Information Protection and Electronic Documents Act — the federal PIPEDA — and also to international European Union directives.

Conversely, here's what PIPA is not. It does not provide broad access rights within the private sector, so an individual only has the right of access to their own personal information. There is no right of access to information about a business, their financial operations, their personnel, etc. It is not a complicated set of rules and regulations that will prevent business from collecting and using personal information for legitimate purposes.

When we wrote PIPA, we tried to write it as a storybook so that organizations could open it and be able to follow, from the beginning, what it was that they needed to do to meet the requirements around personal information. It's not that much different from most of the practices that business had already had in place. We had it confirmed for us, when we went around and met with a lot of the businesses, that most were doing these kinds of things anyway. It's not unique to British Columbia; it's based on an international set of standards.

The historical backdrop. In 1984 the Organization for Economic Cooperation and Development produced guidelines on the protection of privacy and transborder flows of personal data. Canada became a signatory to that document.

In 1996 the Canadian Standards Association issued a model code for privacy that has really formed the basis of all the legislation in Canada that has flowed for the private sector from that point on. This code was developed in consultations with consumer groups, businesses and government representatives.

On October 28, 1998, the European Union passed its directive on data protection. The directive regulates all the data transfers that go between the European Union states, and it prevents data sharing with jurisdictions that do not have an equal level of data protection. A lot of jurisdictions in the world looked at what they

needed to do to be compatible with the European Union directive so that they could continue doing trade and sharing personal information. Canada chose to develop its own legislation. The United States went with the concept of safe harbours.

The federal government brought in its own legislation in response to the European directive, and that is called PIPEDA, as you've heard me mention. It was passed on April 13, 2000, and it was implemented in three stages between January 1, 2001, and January 1, 2004. It is, as I said, based on the Canadian Standards Association's model code for privacy.

[0810]

When the Canadian federal government brought in their act, one of the things that they included in it was a clause that said if provinces didn't develop their own similar legislation within three years, then the federal act would apply to all businesses that are operating within a province. That was the beginning of the provincial government looking at a way of developing legislation for this province.

In 1999 British Columbia struck an all-party special legislative committee to look at information privacy in the private sector. In its report in 2001 it made a number of recommendations. One of those was that the government of B.C. enact legislation to protect the privacy or the personal information of individuals held by the public sector.

Why did some provinces choose to do their own legislation? In Canada, Quebec has provincial private sector legislation, as do Alberta and British Columbia. Those are the only three at this point. Quebec's was in place long before PIPEDA, so it was really B.C. and Alberta that decided to develop their own.

There were three compelling reasons. PIPEDA is very complex and can be a difficult act to interpret. It was felt that in the provincial private sector, where you're dealing with a lot of businesses that are very small — you have a lot of corner stores, mom-and-pop operations — having a piece of legislation where you're having to flip back and forth between various sections wasn't a good regulatory form for them.

If PIPEDA was brought into B.C., it would also leave gaps, so the employees in provincial organizations would not be covered. The federal PIPEDA covers employees in the federal-based organizations but couldn't cover the employees in the provincial bodies. It also did not cover the not-for-profit sector, and it was felt that this was a very important sector. There are an awful lot of organizations that are doing mental health counselling and addictions counselling and that have very sensitive personal information. It was felt that it was important to cover those groups as well.

The other reason was that if you went under PIPEDA, it meant that the province would be subject to the federal Privacy Commissioner. The federal Privacy Commissioner model is very different from the Information and Privacy Commissioner that we have in British Columbia for the Freedom of Information and Protection of Privacy Act. That commissioner, as you're probably all aware, has order-making power.

The federal commissioner for both their public and private sector acts only has recommendatory power — ombudsman-type power. Those were the main compelling reasons for going forward with legislation in B.C.

We held information sessions across the province. A lot of those were booked through the chambers of commerce and the Rotary. There were 17 different sessions across the province. We also held in-depth consultation with over a hundred key stakeholders and stakeholder organizations.

What they told us in the beginning was that they viewed this kind of legislation as just good privacy practices. They could sell it. They could say to the people: "Look. We are following these practices, and therefore we're protecting your information. We're a good business to deal with."

They preferred provincial legislation. They wanted a plain-language statute. You've got to remember, again, as I said, that there are a lot of organizations that are very small, and they didn't want to have to hire a lawyer to come in and interpret the legislation for them or to help them put the tools in place. They wanted the act to be harmonized with other provincial legislation and also the federal legislation. A lot of these organizations have companies in a variety of provinces, and they didn't want to have to be juggling different regimes across the country. They also wanted implementation support, which was provided.

In terms of cross-jurisdictional consistency, when British Columbia had started developing the legislation or its drafts, Alberta asked if they could partner in that process. So the drafters from British Columbia were used. We would draft the legislation here and then share it with Alberta. Alberta would either accept it, or they would change it slightly to fit their needs in Alberta. What you have as a result is two provinces with legislation that is virtually the same.

One of the constraints in developing provincial legislation was that it had to be deemed substantially similar to the federal act, PIPEDA. For British Columbia that occurred on October 12, 2004. There is some consistency between the federal act and the provincial legislation.

[0815]

What does PIPA apply to? PIPA applies to all organizations in the province. PIPEDA, the federal act, only applies to those engaged in commercial activities. That's not true in B.C., where it applies to all organizations. It applies to a person, a corporation, a partnership, a sole proprietorship, an unincorporated association, a trade union and all of the not-for-profit sector.

What it does not include is personal or domestic uses. So if you're using something in your personal capacity for your home or your family, then that's not covered by this legislation. It doesn't cover journalistic, artistic or literary uses. It does not cover the courts. It does not cover a public body that's covered under the Freedom of Information and Protection of Privacy Act. It doesn't cover organizations that are captured by the federal PIPEDA. Otherwise, virtually every organization in British Columbia is covered.

What is personal information under this legislation? The definition is very similar to under the Freedom of Information and Protection of Privacy Act. Actually, I'll step back a second and say that when we were drafting this, we did use the FOI Act, as I'll call it, as a template to follow. You'll find a lot of the sections parallel the FOI Act where possible.

The definition for personal information is very similar to that. It's information about an identifiable individual. This could include anything — like a person's name and address. It could include their social insurance number. It could include information about religion, education, their medical. The definition only says "about an identifiable individual," so it's very broad. It includes employee, and under the definition of employee, that also includes volunteer personal information.

What it does not include is contact information about an individual's business capacity. Say I was operating KLM Electric or something, and I had a business card. The name of my company and my name, if it's on there as proprietor, the address, telephone and fax number all would be called contact information and would not be considered to be personal information under this legislation. If it was my home address as an individual, that would be my personal information.

It also doesn't include work product information. I got a call not too long ago from one of the organizations that's participating in the federal submissions or the consultation process. They had indicated that there seemed to be misunderstanding about the work product, and he had wanted to clarify what in fact we did mean in B.C. by work product. What the work product information means is that if I'm preparing information for my work — letters, maybe information notes, I'm signing contracts, etc. — those are not considered to be my personal information even though they may have my name on it. They are the information that I prepare for the business. So I couldn't go in and say to that business, "I want access to all my personal information," and expect that I was going to get those kinds of documents in response.

The personal information. If I was a social worker and I was preparing a case history of somebody, that case history wouldn't be considered to be my personal information. But the personal information in it is protected under PIPA because it's the personal information of the subject of the report. It's just not my information as author of the report.

I hope that's clear. It's a little bit of a convoluted definition, but it's really meant to ensure that individuals who are authoring documents don't expect that those will be their personal information.

As I mentioned in the historical backdrop, this legislation, as are the other ones in Canada, is based on the Canadian Standards Association model code. It has ten principles. They're listed on the slide in front of you. What we're going to do is go through each one of those principles very briefly. I won't list the ten of them; I'll just go through them as we get to them.

The first one is identifying purposes. Under PIPA an organization must identify either verbally or in writing

what the purposes are for the collection of the personal information and how they're going to use and disclose that. They've got to tell you up front. The purposes must be reasonable and appropriate in the circumstances. That's one of the things the Information and Privacy Commissioner can review: whether or not what you're doing is reasonable in the circumstances.

[0820]

Examples of the collection of personal information are if you're opening an account somewhere — at a credit union, for example; if you're going for counselling, you have to provide basic information for those services; if you're becoming an employee, you have to provide information for the individuals in order to enrol you in whatever programs and benefit programs, etc., they have. But they have to know up front why it is that they're providing this information and what you're going to do with it.

PIPA requires that there are limits on the collection of personal information. The organization can only collect personal information that is reasonable in those circumstances. If somebody were to go into an organization and the company said they were setting up a cell phone and were asking for their income or their social insurance number, they could go back and question if that is reasonable in these circumstances and decide whether or not they're going to provide it.

Information must be necessary to fulfil the identified purposes — again, that comes back to the reasonable test — or where it's otherwise permitted under PIPA. There are a lot of instances, which we'll talk about in a minute, where you can collect personal information without the consent of the individual.

There are just a couple of examples there that we have already talked about. Would an organization need your level of income or your education if you are taking out a warranty card at a store, for example? Would they need your social insurance number if you're using your credit card? Different things like that.

PIPA is consent-based, so it's very different from the Freedom of Information and Protection of Privacy Act in that instance. There are three forms of consent under PIPA. The first is explicit consent. That's where the organization is going to tell you exactly why they're collecting your information. As I said, they can do that verbally or in writing.

Then they are going to get you to explicitly — I hate to go back to using the term again — give your consent. So you're either going to sign in writing that you have given your consent, or you can provide it verbally, and then they would document that at the other end. That's where you know exactly what it is they are collecting the information for. That's the most common form of consent and should be the one that's relied on most within businesses and not-for-profit organizations.

The second one is implicit or deemed consent. In that case, the purpose must be obvious, and the information is supplied voluntarily. If I'm phoning up TicketMaster and I want to buy tickets to the Rolling Stones, it's assumed that they're going to use — of

course, if it's by phone, I pay by credit card — my credit card information in order to put my charges through, and that they're going to use my address, etc., to mail the tickets to me if that's the option I've chosen. That's what the implicit or deemed consent is about.

Oftentimes you'll find implicit consent used in the medical field. If you go in and have a blood test done, as would have been ordered by a doctor, then it's deemed that you will want that blood test sent back to the doctor that referred you there to get it. That's where you'll find implicit consent as well.

The third consent is an opt-out consent. I know that most of you will have encountered these when you get something in the mail and they say, "We'd like to use your information for marketing purposes or something else," and they'll have a little check box. You either check off that you agree to that, or you don't. If they have sent that out, asked you to check, and they don't hear from you or you don't check the box, then they can assume that you didn't opt out and that you're okay with them using that information.

There are also instances — it's not a type of consent — under the act where no consent is required. There are circumstances where an organization can collect, use or disclose personal information without the consent of the individual. Some of those are listed: if there's a medical emergency; if it's necessary to collect a debt; if it's in the individual's best interests; if the information is publicly available through a telephone directory; if it's for an investigation, for example, where to get their consent would then impede the investigation. There are those kinds of options.

Some constraints on the consent provision. Consent is not valid if it is collected by deceptive means. An organization couldn't lie about why they were collecting the information and then have that consent remain valid. It can also not be made a condition of supplying a product, if the information gathered is beyond what is necessary or reasonable to provide that product. Withdrawal of consent cannot be prohibited unless it would frustrate the performance of a legal obligation.

[0825]

The PIPA distinguishes between personal information and employee personal information. The reason for this was that it was based on the fact that in most instances the employee circumstances are not ones of consent. What the act says is that organizations can collect, use and disclose employee personal information without the employee's consent if it's for reasonable purposes that are related to the establishment, management and termination of that employment relationship.

They can't collect other information about the employee without their consent that is beyond those confines, but for that purpose, they can. They do, however, have to notify the employee that this collection is going on. The employee has the right to see that it's reasonable and to question it if they don't believe it is. Again, there are some limited circumstances where that notification wouldn't have to be provided, and that is where there are medical emergencies or where there is

an investigation or proceeding where it would impede that investigation.

One of those things that B.C. put in PIPA that is different than the federal legislation is a section in there that relates to the sale or merger of a business. What businesses had told us was that oftentimes when they're selling a portion of their business, the company that's buying it needs to see the information about employees, about customers, that sort of thing. Under the federal act they couldn't do that.

This allows the organization to disclose information about their customers and about their employees, directors, etc., to a prospective purchaser. There are very strict criteria around how they can use that information and how they can disclose it, and the retention period. If a sale doesn't go through, then that information has to be returned or destroyed, for example. They also can't use it for secondary purposes. But it does allow them to evaluate the business and see whether they're going to take it on.

A business can't sell just its customer list. They have to be selling a substantive part of the business, of which the customers are a part. The new business — if they do buy the business, and the new one takes it on — can use that information for the same purposes that the first businesses were using it. If they're going to take it and then say, "Wow, we've got a brand-new product," or "We want to take our business off on these lines," they would have to go back and get consent from those people to use the information for those purposes. So as I said, there are some tight constraints on the purposes for which that information can be used.

Under the legislation, as I mentioned, there are limits on collection. The collection portions are set out with the basis for collection and then the reasons that you can collect without consent. The use and disclosure provisions under the legislation parallel that. They're set up almost identically. The reasons that exist under each, for when you can collect, use and disclose without consent, are almost the same.

We were asked when we were developing it: "Why don't you just say it once?" We said that for an organization that's using this — again, we wanted to go back to that storybook kind of feel, that they can go through and they don't have to flip back to collection to see what they can do for use and disclosure — it's actually written right there for them.

Consent for use and disclosure must be obtained except in limited circumstances. If you're going to use it for secondary purposes or disclosure, you have to regain that consent. You can't, once you've got consent, then go on and use it for other reasons.

I think that's about all. Let's see. We've already said what the reasons were that you could use without consent under collection.

The PIPA requires reasonable security, so an organization has to make sure, depending on the sensitivity of the organization, that they have appropriate security in place. That would mean physical measures, like you're locking your file cabinets; you're restricting

access to offices. You've got technological measures like passwords, or you've got organizational measures so that people only get information on a need-to-know purpose. Your accountant may not need to know medical information of employees who have come back to work, for example.

[0830]

The PIPA also requires accountability, so the organization has to appoint a privacy officer or somebody to fill that kind of position. That person has to be able to answer questions from the public. They also have to be responsible for all the information that's in their control. So that not only means the information they have right in their custody, but all of the information that contractors may have who are acting on their behalf. They have to make sure they maintain that information to the standards that are set out within PIPA. In most circumstances, the contractors will also be covered under PIPA. But if an organization is using contractors outside the province, they would have to ensure that those contractors meet the requirements of PIPA.

PIPA requires that an organization is open and transparent. To do this, they have to have written policies in place — what their privacy policies are. These policies have to address their obligations under the legislation, and they have to provide these policies to people if they request them. They should have personal information collection notices and brochures that tell what their privacy policy is.

Shortly after we had begun working with businesses on the Personal Information Protection Act, it would be interesting to go into businesses. You would see that right by the cash register they'd have a little privacy policy on a bookmark kind of card. You will see these kinds of policies when you get bank or credit card statements. They just about always have a privacy policy statement in with your bill.

PIPA also requires accuracy. Now, this would be the same as under the Freedom of Information and Protection of Privacy Act, especially if you're using the information to make a decision about the individual, or if you're sending that information or disclosing it to another organization. Again, you have to take reasonable steps to ensure the accuracy of the data you have.

PIPA also has retention stipulations. One is similar to the Freedom of Information and Protection of Privacy Act. That is, that information has to be kept for one year if that information has been used to make a decision about the individual. There is one additional stipulation in PIPA, and that is that information that is no longer necessary for the purpose for which it was collected needs to be destroyed, unless it is needed for other legal or business purposes. You may not need it for the original purpose, but maybe you need it for taxation purposes or something. Then you could keep it longer. But there is a requirement that you destroy information when it is no longer necessary. That's personal information.

The access rights under PIPA, as I said at the beginning, are only for an individual's own personal

information. So a person can ask for their information, or they can ask for somebody else's if they're acting on that person's behalf. PIPA does have a regulation on who can act for others.

It does have similar requirements as under the Freedom of Information and Protection of Privacy Act. The request must be in writing. The organization has a duty to assist. You must respond within 30 days, unless there are reasons for an extension — if there is a high volume of records; if you need to consult with third parties; or if the individual hasn't clarified, to a reasonable level, to allow you to go and look for the records that are being asked for.

An organization also has to provide reasons for refusal in a letter to the applicant, and there are exceptions to that right of access. Those exceptions are fairly limited, but if they would reveal personal information about another individual, then it's a mandatory exception. They must withhold that information. If it were to reveal the identity of a person who has provided an opinion about another person, they must withhold that. They must withhold it for health or safety concerns about the individual or another. They may withhold it for solicitor-client privilege or for confidential business reasons, if it would harm organizations' competitive process. So there are two sets of reasons. One is discretionary, and then those where it would affect the privacy of another individual. Their safety is mandatory.

The access rights also differ from the Freedom of Information and Privacy Act in a couple of ways. In addition to providing the person with the information, an organization must also tell them how their information has been used, and they must also tell them to whom they've disclosed that information. They have to provide those two extra pieces of information in response to an access request.

[0835]

Under PIPA an organization cannot charge an employee for access to their personal information, but they can charge a customer for their own personal information. The charges must be minimal, and they have to issue a fee estimate. The individual may provide a deposit. They're not required to provide a deposit, but they may require a deposit.

They must not disclose personal information. This is different than the FOI Act. Under the Freedom of Information and Protection of Privacy Act, there's kind of a balancing that occurs. You're looking at whether it would be an unreasonable invasion of privacy. That balancing doesn't occur in PIPA. If there is personal information about another individual, then that information doesn't go out even if it means the person doesn't get their own personal information. So there is no balancing in there. It's a much stricter test than under the FOIPPA Act, as I will call it from now on.

There's also correction and annotation under PIPA. An individual can ask for a correction, and if the organization feels that it's reasonable to correct it, they can correct it. They must notify every other organization that they have disclosed that information to over the

past year that that correction has occurred. If they don't believe that there's enough information to warrant the correction, then they will annotate the records.

To annotate means that they will put the correction request on the document where the item is that was requested to be corrected, and they will staple the two together. Anybody coming along will read both of those documents and see what correction the individual asked to have made.

There is recourse and oversight under this legislation. An organization is required to have a process in place to respond to complaints. They are the first level of the complaint process, and they must document what that process is. It needs to be one that's very straightforward and easy to use.

The commissioner has the same role under this legislation as he does under the Freedom of Information and Protection of Privacy Act. Some of the provisions that are in PIPA are a little more modern. There is a look at doing consistency between the two pieces of legislation. His oversight provisions are the same. One of the things that he has in this legislation is that he can require an individual who is complaining about a company to go back to the company and try and resolve it, which is again why the company has to have a complaint process in place — so that resolution can proceed.

There is a grandfather clause under this legislation. It does not apply to information that was collected on or before the act came into force. If a company has a lot of information.... Say you belong to a golf club and they had collected your information in the 1990s. They didn't have to go back and ask your consent to have that information and to use it for those purposes for which they collected it. If they were going to use it for additional purposes, they would now have to ask consent. Any of the other provisions in the act — the security; the new uses, as I've just said; the new disclosures, etc.; and the right of access — all apply to that information, but they wouldn't have to go back and ask you for consent to have it.

As I mentioned at the beginning, we did do implementation initiatives. They were fairly extensive with this piece of legislation. We do have a designated webpage that individuals can go on to. They can get a lot of information from that.

We have a privacy help line. This gets used very regularly. It's manned by an individual between office hours. We get a lot of companies calling in on a daily basis asking for information on how they do a certain thing.

We do regional training. We did a lot of training after the legislation was brought in. We went around the province, I think, for close to a year doing training for community groups, business groups and just for individuals who wanted to be a part of those. They were very well attended. We just did a training session last week in Victoria, and we have one in June in Vancouver. We don't do them as much anymore, but we are doing them sporadically.

We do have guidelines and tools. I have given you a package. On the next slide there is a listing of what

those guidelines and tools are. What we tried to do is really do a step-to-step how-to for businesses so that they could go to these tools and they could walk themselves through what they needed to do in order to be compliant. So you'll notice it says: "How do I know if I'm covered? What is a privacy officer? What are the ten basic principles that I have to follow in order to meet the requirements of this?"

[0840]

You'll see that the next one says: "Conducting a privacy audit." A lot of organizations didn't know what personal information they even collected. We suggested that they do an internal privacy audit. This gives them directions on how they can do that themselves. Then there was a privacy compliance assessment tool, which allowed them to check off the boxes to see if they were compliant; setting up a complaint handling process; a model privacy policy, so they could just fill in the blanks, that kind of thing; and then model contract language. I've given you a handout of all of those implementation tools so that you can take a look at them.

There were some amendments done to PIPA. There were some done shortly after it was implemented. A lot of those were basic grammatical changes, wording changes after an initial draft — there were a few of those.

There were some provisions brought in, though, that allowed the commissioner to interact with other commissioners who were also dealing with issues under private sector privacy. A lot of the issues seemed to span all jurisdictions. You might have a business that's operating in B.C., but they might fall under PIPEDA because they're doing cross-jurisdictional data sharing. This allows the commissioners to communicate to see who would be best able to hear that particular complaint.

The most substantive amendments were brought in 2006. One was around solicitors' liens. We had been contacted by the Law Society and the Canadian Bar Association around solicitors' liens. One of the things they indicated to us was that a lot of times when they get personal information about an individual whom they are assisting in a legal way, they collect a lot of information. Sometimes that individual will leave and either go to another lawyer or decide to pursue the issue on their own. They will ask for all the information and the lawyer's notes, etc., around that case, without paying the lawyer's bill. And so....

L. Krog: I am shocked. [Laughter.]

S. Plater: I can tell that you're shocked.

M. Polak: He was appalled.

R. Cantelon (Chair): Order, order. Get him some water.

S. Plater: What they said was that if PIPA was going to allow those people, then, to get all this information for free, or under the legislation to ask for this information at a minimal cost, this would really be contrary to how the legal profession operates. They

said it could also be detrimental to individuals who are of lower income or who are vulnerable, because what might occur is that lawyers would insist on costs up front in a lot of cases, and people might not be able to pay those, especially if it was a long-term injury case or something like that.

So what we did was bring in an amendment saying an individual can't request their own personal information if the information is in a document that is subject to a solicitor's lien.

The other change — this one is quite complicated — applies to collection, use and disclosure. It applies to the three, across the board. This related to information that was collected in, say, counselling or a medical area. It also applied in the legal area.

When you go in to a counsellor, for instance, you have to provide a whole pile of information. You're providing your case history, or sometimes you may be going to see them about an issue between yourself and another individual, so you will be divulging information about that individual. Under PIPA, the counsellor or the medical professional doesn't have the consent of that other person to collect their information, yet in a lot of cases it's imperative, to be able to understand the person you're helping, that you have that information. The counsellor — we'll use that as the example — may also need to disclose that other person's information if they're sending their client for further testing or assessment.

What the amendment does is say that the counsellor, medical doctor or lawyer can collect that information if it's necessary to provide the service to the person that's providing it to them — if it's necessary to provide the services to their client. That's a little convoluted.

Now, as I mentioned before — or maybe that was before we turned the mikes on; I'm not sure — the House of Commons Standing Committee on Access to Information, Privacy and Ethics recently did a review of the federal legislation, PIPEDA. They've just issued their report, on May 2, and there are a number of instances in their report where they have made recommendations that would move PIPEDA closer to PIPA, so I just thought I'd highlight those to you.

[0845]

They recommend that PIPEDA be amended to permit businesses to collect, use and disclose information without obtaining prior consent, for the purposes of business transactions such as mergers and acquisitions. I had indicated that PIPEDA didn't have that and we put it in PIPA, and they've made a recommendation for that.

They've also recommended that PIPEDA include the definition of "work product." They've recommended that the definition of "business contact information" under PIPEDA be expanded to include faxes, e-mails, etc. PIPA does have those in its definition.

They've also recommended that their consent requirements be clarified and the distinction made between the three categories of consent. They call their categories of consent something different, but PIPA

does have the three categories, and PIPA does distinguish between them and labels them clearly.

They also recommended that PIPEDA be amended to add other individual, family or public-interest exemptions to make it compatible with Quebec, B.C. and Alberta. So there are a number of instances where it will be moving closer to what PIPA has.

That's it for my presentation.

R. Cantelon (Chair): Questions?

L. Krog: With respect to the issue of openness and under that section, it struck me that probably a lot of businesses in British Columbia don't actually comply, have policy — haven't ever taken that step. I'm thinking of small operations — three or four employees, a family business.

What sort of enforcement is undertaken?

S. Plater: The commissioner has the right to review all businesses, so if somebody complained to the commissioner and said, "I know this company, and they don't have the privacy policy," he could initiate an investigation.

There are offences under the legislation, but most of those are for if they impede the investigation or if they don't follow the orders of the commissioner. However, there is the right to sue under this legislation.

If an order were to be issued by the commissioner and it were to go through all of the appeals and be finished and an individual was deemed to be disadvantaged by that order, they then would have the right to proceed through the courts with that.

We try to get as much information out there to all those businesses, but we recognize that we won't reach all of them. That's why we use our website so extensively — so that organizations can go up on the website.

I think this legislation is meant to be remedial, as well, so that if somebody does get a complaint, what can happen, hopefully, is that they can then be instructed as to what their requirements are.

The implementation tools do make it pretty easy for them to do a privacy policy, for example. It's a template. They just have to fill in the blanks.

L. Krog: Do you have any statistics about complaints that are made or lawsuits that have been successfully launched around...?

S. Plater: I don't. The commissioner's offices will have the number of complaints. I don't believe there have been any lawsuits. In our office we don't hear many complaints about PIPA. We get people calling in and asking questions on implementation, but we don't hear many complaints. But the commissioner would be able to tell you that, yes.

L. Krog: Thank you.

R. Cantelon (Chair): Any other questions?

Are there any other pending suggestions for legislative changes that have come up?

S. Plater: We don't have any at the moment. The ones that we wanted to do were made in 2006. We don't currently have a list. Often we do. Around the Freedom of Information and Protection of Privacy Act, we're always getting suggestions in.

Well, we currently have one that just came up in the last day around PIPA, but I still have to evaluate to see whether that's one that actually is an amendment base. But no, we don't have a backlog of changes either that we want to move forward or that have come to us from other parties.

R. Cantelon (Chair): We'll have ample time to give you time to consider that and bring it forward.

H. Lali (Deputy Chair): I have more of a comment than an actual question. My understanding is — and I know from my own personal experience having to deal with organizations or companies, etc., or even if you're renting an apartment from somewhere — that most people don't know that organizations, businesses and individuals are not allowed to ask certain information. At the same time, those organizations and companies and individuals often don't know that they can't ask that kind of information.

[0850]

Really, it's an issue of awareness and education. So I guess the question would be: how do we overcome that? Any suggestions around that? You're looking at tens of thousands of businesses and hundreds of thousands of individuals involved in this.

S. Plater: I think the basic suggestions for overcoming that would be getting the information out to the chambers

and to the business organizations which these may be affiliated with. Now, that's not going to get everybody. Rotary clubs are what we used in the first place. It's going out through those venues where people might be attending where they're likely to hear about this information and then directing and maybe putting out new mailouts or bulletins, etc., that this information is out there.

I think one of the things with our privacy help line is that that phone rings a lot every day. It's usually new businesses that have discovered that the legislation occurs, and they are going: "What does this mean to me? What do I have to do? I've got this employee, and I don't know how to approach this." I think that having that privacy help line there is a good way of assisting those businesses.

Like you say, it's getting the information out there to tell people that it's happening and, I think, possibly going back out through those business organizations and the retail association, etc. — like that. Putting new bulletins out in newsletters and that sort of thing is probably the best way.

R. Cantelon (Chair): Seeing no other questions, thank you very much, Sharon, for coming and filling us in. We may reserve the right to ask follow-up questions once we've digested this considerable material.

S. Plater: You're welcome.

R. Cantelon (Chair): We have the next meeting scheduled for May 29 at 8 a.m. with Mr. Loukidelis, and we'll be reviewing the commissioner's role.

If there's no further business, a motion to adjourn?

The committee adjourned at 8:52 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.