



Third Session, 38th Parliament

---

REPORT OF PROCEEDINGS  
(HANSARD)

---

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

**Victoria**

**Wednesday, February 6, 2008**

**Issue No. 5**

RON CANTELON, MLA, CHAIR

ISSN 1913-4746



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

Victoria  
Wednesday, February 6, 2008

*Chair:* \* Ron Cantelon (Nanaimo-Parksville L)

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

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

*\*denotes member present*

*Clerk:* Kate Ryan-Lloyd

*Committee Staff:* Josie Schofield (Committee Research Analyst)  
Stephanie Hansen (Administrative Assistant)

---

*Witnesses:* Bart Armstrong  
Sheldon Greenspan (NAID Canada)  
George Hancock (United Auto Trades Association of B.C.)  
Robert Johnson (Executive Director, NAID Canada)  
Laura Knight (Insurance Brokers Association of B.C.)  
Dave Morgan (Galiano Club)  
Mandy Parker (Association of Fundraising Professionals for Vancouver  
Island)  
Roger Phillippe  
Gerry Preddy (Vice President, United Auto Trades Association of B.C.)



**CONTENTS**

Special Committee to Review the  
Personal Information Protection Act

Wednesday, February 6, 2008

	<b>Page</b>
Presentations .....	27
S. Greenspan	
R. Johnson	
B. Armstrong	
R. Phillippe	
M. Parker	
G. Preddy	
G. Hancock	
L. Knight	
Next Committee Meeting.....	37



MINUTES

# SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT



Wednesday, February 6, 2008  
1 p.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 meeting to order at 1:03 pm.
2. Opening remarks by Ron Cantelon, MLA, Chair.
3. The following witnesses appeared before the Committee and answered questions:
  - 1) NAID Canada Sheldon Greenspan  
Robert Johnson
  - 2) Bart Armstrong
  - 3) Roger Phillippe
  - 4) Association of Fundraising Professionals for Vancouver Island Mandy Parker
  - 5) United Auto Trades Association of British Columbia George Hancock  
Gerry Preddy  
Laura Knight
  - 6) Insurance Brokers Association of British Columbia
4. The Committee recessed at 2:14 p.m.
5. The Committee reconvened at 3:00 p.m.
6. As no further witnesses were present, the Committee adjourned to the call of the Chair at 3:03 p.m.

---

Ron Cantelon, MLA  
Chair

Kate Ryan-Lloyd  
Clerk Assistant and  
Committee Clerk



WEDNESDAY, FEBRUARY 6, 2008

The committee met at 1:03 p.m.

[R. Cantelon in the chair.]

**R. Cantelon (Chair):** Good afternoon, ladies and gentlemen. I'd like to welcome you this afternoon to this meeting of the Special Committee to Review the Personal Information Protection Act. My name is Ron Cantelon. I'm the MLA for Nanaimo-Parksville, and I serve as Chair of this parliamentary committee.

Our committee has been asked by the Legislative Assembly to review the Personal Information Protection Act, as per the act itself, which requires that every six years the act be reviewed by a special committee — an all-party committee — of the Legislative Assembly. We are holding a public hearing today here in Victoria, and we will be accepting written submissions on this subject until February 12, 2008.

Today we have seven individuals who have registered to speak with us. Prior to hearing from the first witness, I would like to ask the committee members to introduce themselves, starting with the member on my right.

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

**L. Krog:** Leonard Krog, MLA for Nanaimo and vice-Chair of the committee.

**R. Cantelon (Chair):** I've introduced myself. I would also like to introduce the committee staff present with us today. Everything that is said will be recorded and transcribed by our Hansard staff. Behind us we have Wendy Collisson, Polly Vaughan and Graham Caverhill. We are also joined by our community assistant Stephanie Hansen at the back of the room, by our researcher Josie Schofield and by Kate Ryan-Lloyd, who is Clerk Assistant and Committee Clerk.

The committee has been asked by the Legislature to review the Personal Information Protection Act and, specifically, the collection, use and disclosure of personal information by private sector organizations. We are mandated by the Legislative Assembly to report back no later than April 19. At that time we will submit a report which will likely include consideration of the committee recommendations on how to improve the act itself.

[1305]

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

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

In addition to the meeting transcript, a live audio webcast of this meeting is also produced and available

on the committee's website to enable interested parties to review the proceedings.

Again, I'd like to thank you for coming. Our first presentation this afternoon is Mr. Robert Johnson and Mr. Sheldon Greenspan of NAID, which is an acronym for the National Association for Information Destruction in Canada.

I'd just like to acknowledge we have John Rustad. John, if you'd like to identify yourself.

**J. Rustad:** Hi. I'm John Rustad, MLA for Prince George-Omineca.

**R. Cantelon (Chair):** He joins us electronically. Gentlemen, if you'd like to proceed.

### Presentations

**S. Greenspan:** On behalf of the National Association for Information Destruction, NAID Canada, I would like to thank the committee for the opportunity to speak here today. My name is Sheldon Greenspan. I was the founding chair of NAID Canada, and I continue to sit on the board of directors. With me is Robert Johnson, the executive director of NAID Canada and our sister associations in the U.S., Europe and Australasia.

We will also be making a written submission to this review that elaborates on the remarks made here today.

NAID Canada is a non-profit trade association for the secure information and document destruction industry. NAID Canada's members provide commercial services ranging from the secure shredding of discarded paper records to the destruction of information contained on end-of-life electronics.

NAID Canada and its sister associations in other countries have also earned a reputation as a vigilant consumer advocate and as a trusted and credible resource for policy-makers. There's a growing understanding among policy-makers around the world that protecting personal information at the end of its life cycle is every bit as important as protecting it during its useful life.

British Columbia has been a leader in Canada on this front, with section 35(2) of PIPA requiring organizations to destroy documents containing personal information as soon as is reasonable. First and foremost, we congratulate the B.C. government for including such a clause in PIPA.

Our comments today will be focused on making that clause more powerful by including a definition of destruction in the legislation itself. It is the same recommendation that we have already made in the reviews of PIPA in Alberta and with PIPEDA federally and for which policy-makers have generally offered their support.

Why add a definition of destruction if it is already required in the legislation? NAID Canada offers two reasons in response to that question.

First, while destruction is required under PIPA, and while it certainly seems like common sense that discarded personal information should be destroyed first, this is not happening. There are media reports literally

every day about privacy breaches resulting from unsafe information destruction practices. These range from documents left in dumpsters or recycling bins, where they are easily accessible to the public, to information being left on old computers or other electronic equipment slated for reuse or recycling.

We contend that such cases partly result from a lack of clear direction on what exactly destruction means. Recycling, for example, is not destruction. Documents may still remain intact, vulnerable to a privacy breach, for extended periods of time before being recycled. Throwing records in the garbage is obviously not destruction.

However, even some types of shredding are not entirely safe. In fact, we often joke that bags of shredded documents in the dumpster or a recycling bin are a gift to identity thieves because they must contain the most useful information. Sophisticated criminal elements will invest the time to put this information back together if it is shredded poorly.

The truth is, these incidents are unique only in the fact that they make headlines. On any given day it would not take long to find personal information being discarded intact and accessible to the public.

[1310]

Therefore, NAID Canada recommends adding a definition of destruction in section 1 of PIPA. Destruction should be defined as the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information or parts thereof is not practical.

According to a study conducted in the United States, the vast majority of identity theft results from low-tech access to personal information, such as dumpster diving or binning. Indeed, law enforcement officials in the U.S. recently exposed elaborate rings of organized criminals capitalizing on this ready source of personal information. These rings were found to have divisions of labour where lower ranks started by harvesting the information from dumpsters, which is then handed over to others of higher rank who have been trained to best exploit it.

Our message is clear. Privacy protection is no longer simply a human rights issue. Violating the rights of others by casually discarding their personal information provides much of the feedstock for what has become a global epidemic of identity theft.

Only in the United States has a new generation of legislation begun to appear, exemplified by FACTA and a host of state laws which are designed not only to protect privacy rights but also to stem the tide of identity fraud. As a result, there is a marked difference in the regulatory language regarding information disposal.

Where in the past a regulatory reference to information disposal would require limiting unauthorized access, improved regulations now require that steps be taken to destroy personal information prior to its disposal. Further to the point, the new generation of legislation requires that security measures be documented in the organization's policies.

We are here to respectfully urge this committee to enhance the effectiveness of PIPA in protecting the citizens of British Columbia by adopting a similar

approach. Information destruction requirements must be clearly spelled out in legislation. That is the only way to put an end to these unnecessary breaches.

Now let me turn to the second reason for adding a definition of destruction to PIPA. Doing so will send a clear message to all organizations that information destruction must be taken seriously. It is clear from the regular reports of breaches resulting from unsafe destruction that many organizations are not paying attention to this area of privacy protection. This is extremely dangerous. All the steps taken to protect information during its useful life are undermined if safe destruction practices are not implemented when the documents in question are no longer needed.

Section 5(a) of PIPA requires organizations to document their privacy policies. By adding a definition of destruction to PIPA, the B.C. government can force all organizations to re-examine their destruction practices to ensure that they are providing the highest standards of protection to the public.

When making this recommendation in other jurisdictions, it has been alleged that this will create a new burden for business. This is not a valid argument, in our opinion. Organizations should already be using safe destruction practices. If they are not, investing in doing so and documenting it is far less costly than having your company name all over the media because you're responsible for personal records falling into criminals' hands.

The B.C. government, along with the Information and Privacy Commissioner, could use this legislative change to launch a public education campaign about the importance of safe destruction, especially at a time when so many people are falling victim to identity theft. It would certainly put B.C. well ahead of any other Canadian jurisdiction.

Adding a definition of destruction is our only specific recommendation. It may seem mundane or possibly even redundant, but it is critical to privacy protection and information security.

I would just offer general comments in two other areas. First, we support stronger contracting requirements between information custodians and third parties to whom destruction is outsourced. For example, NAID Canada is a professional association. Our members must abide by certain standards. We also have a rigorous certification program for members who want to be recognized as the top of the class in the information destruction industry.

When such professional standards exist, we believe they should be recognized by policy-makers — if not in legislation or regulation, then certainly by enforcement bodies like the Information and Privacy Commissioner.

[1315]

Second, we support breach notification laws, which has been a hot topic lately. Historically, such notification has been reserved for incidents involving sensational electronic data breaches. It is important to note, however, that a breach resulting from casual disposal of paper records can be just as damaging for customers and consumers. Therefore, if PIPA is going to be amended to include a notification requirement for

electronic data put at risk, such a provision must also exist for the casual disposal of paper records.

In closing, I wish I could tell you that your good counsel and prodding would be enough to prevent the casual disposal of personal information, but history has proven that more deliberate direction is required. Privacy legislation must define information destruction.

We thank you for the opportunity to appear before you today. We firmly believe that if British Columbia acts on our recommendations, this province will have some of the highest information protection standards in North America. We remain at your service at any time to provide further input or support for this committee's efforts to better protect the privacy of British Columbians.

**R. Cantelon (Chair):** Thank you for your presentation. I have a couple of questions, but I'd first like to acknowledge and recognize that the hon. Harry Lali, the member for Yale-Lillooet and Deputy Chair, has joined our committee.

Thanks, Harry, for being here.

**L. Krog:** Mr. Greenspan, thank you very much for the suggestions. I think they're very valuable — not that I want to presuppose what I would recommend to the committee as a whole. But having said that, I presume there's some precedent in other jurisdictions for this.

**S. Greenspan:** Absolutely. Bob, would you like to take that?

**R. Johnson:** As far as precedent, as you may know, PIPEDA as well as Alberta's PIPA are currently under review. PIPEDA is a little further along. Both of the committees to which we've made a very similar presentation have adopted this recommendation and forwarded it on as something that was.... So in that regard, in Canada it has been addressed — or that's the extent to which it has been addressed with regard to adding a definition.

In the U.S.A, FACTA, which stands for the Fair and Accurate Credit Transactions Act, has within its 19 provisions one provision that's called the "final disposal rule." That rule, which requires the destruction of credit bureau information or consumer reports, as they call it, does actually spell out what destruction is — and it's a very similar definition — as well as requiring that written policies and procedures be in place and that a contract exists between any service providers. So there's an element of due diligence with regard to selection of a service provider as well.

I would also say that the Health Insurance Portability and Accountability Act in the U.S. also has a provision that requires that any third party contracted to handle personal information must have a contract agreeing to the provisions of that as well. So the other is precedent, I guess.

**M. Polak:** That question has been dealt with, so my second question left is relatively simple. You ask that the improved and increased professional standards be recognized by policy-makers and/or by the Informa-

tion and Privacy Commissioner. What do you mean by that? How would you see them being recognized?

**R. Johnson:** I'll take that too. Again, referencing some precedent in what that might look like, with regard to the Fair and Accurate Credit Transactions Act, the United States Federal Trade Commission, during the rule-making process in the legislation, specified that one aspect of due diligence in the selection of a contractor to destroy information would be that they be certified by a nationally recognized trade association. NAID being the only such trade association, it was a de facto reference to ours.

The only other direct reference that I can think of, per se, is that Dr. Ann Cavoukian, the Information and Privacy Commissioner for the province of Ontario, has issued a publication in response to a pretty interesting breach that came about from casual disposal. In fact, her first executive order under their PHIPA regulation.... She produced a fact sheet wherein she recommended that any contractor that was selected to destroy information be made certified. So she actually specifically recommended NAID's certification in that publication.

**M. Polak:** So it's recognition regarding the certification that you would provide then.

**R. Johnson:** Exactly. Yes.

[1320]

**H. Lali (Deputy Chair):** I, too, want to join my colleagues in saying these are very good recommendations and suggestions that you have made in front of the committee here.

You talk about identity theft, and you basically use the United States as an example where most of the identity theft, as you say, occurs. People are actually throwing out records rather than destroying them, and then dumpster diving, etc. Do you have any idea if it's similar here in Canada as well? You just mention the United States here in your report.

**S. Greenspan:** It's a global epidemic. There is such a plethora of examples of situations happening in every province and in every city.

**R. Johnson:** I'm not sure that there has been any research done per se in Canada to determine what the root sources are. Of course, the raw material it takes to commit identity theft is the personal information wherever it is accessible. The Javelin study, which is referenced there, was conducted with the Better Business Bureau and the Javelin group and I think another group called the penom group, that did show it was low-tech access to information, such as dumpster diving, that was the major source of that. I do believe that was relegated to the U.S., but Sheldon's point is well taken in that it's pretty much the same MO everywhere. They're going to go where it is and where it's easy.

One of the other interesting phenomena we've also seen — it's just an aside, if I may — is that because identity theft is largely a borderless crime, where jurisdictions like the U.S. start imposing more restrictions, you find these people who are adept at this going to places where the legislation is lax. So it's a bit of a self-defence mechanism that you want to stay up with the latest prevention methods. Prevention is really the only true.... Apprehending or detecting this crime is very tough.

**M. Polak:** One more quick question. In taking a look at the section that exists in 35(2), it says: "An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals...."

From your perspective, how does the use of the word "obliterate" and the other phrasing that you use in your recommendation improve the existing situation?

**S. Greenspan:** Because it defines it. You can interpret the wording, as it presently stands, a multitude of different ways. We've tried to be very clear in our definition whereby "physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information or parts thereof is not practical."

A lot of time and effort was spent, in terms of coming up with this definition, not mandating a specific process and also trying to allow the flexibility, depending on the media and the technologies in the future. The key point of obliterating the information so that it is no longer relevant and useful is really the key concept.

**R. Johnson:** If I may add to that as well and maybe to make the most dramatic case for a reason for a definition. It might even sound ridiculous to you here, but we hear it. That is that someone will defend their practice of putting that information in the dumpster because eventually that dumpster is dumped into a truck, that truck is taken to the landfill and that stuff is put into the landfill and buried. "That's our destruction, so it complied with the law, thank you very much."

Their interpretation of what is destruction leaves a lot of room for creativity. Certainly, you or enforcement officials would have the right to a reasonable standard in that regard. I think we all agree that's not reasonable, and yet it's still out there as a possible interpretation.

**M. Polak:** Thank you. That illustration helps too.

**R. Cantelon (Chair):** Seeing no further questions, I'd like to thank you gentlemen for coming in and making a very direct and cogent presentation. It's very useful to the committee, and we look forward to your written submission to support what you told us today.

The next witness I'd like to call forward to the table is Bart Armstrong, an individual who wishes to make a presentation. We understand that he'll be submitting written material following his presentation.

Mr. Armstrong, you have the floor.

**B. Armstrong:** Before I start my presentation, I would like to just add something from the last presentation. I have personal hands-on experience with dumpster diving — not me doing it; I'd better change the way of wording this. Collection agency documents that were thrown in dumpsters and the wind got a hold of it and blew it all over the place. This was in the province of Nova Scotia, and I would encourage this committee to communicate with the people in Consumer Affairs Nova Scotia. You can get lots of information about silly antics in Nova Scotia. This is a few years ago, mind you.

My name is Bart Armstrong, and I live in Victoria, British Columbia. I'm presenting this brief unofficially on behalf of about 551,000 households and well over one million renters in British Columbia. I would like to thank the Chair and committee for hearing me today.

About one in three households in Canada is a rental unit. Approximately 94 percent of these 4.2 million households enjoy a privacy right that we in B.C. do not have. PIPA has now been with us for about four years. It has levelled the playing field. It now requires private organizations to rise to the bar of acceptable standards by government agencies with regards to the privacy information of individuals.

Here in B.C. there is a flaw that allows landlords to violate the basic right of privacy mandated by PIPA and, in so doing, releases for public consumption very private and personal information. I refer to the common practice of landlords posting notices on the doors of their tenants. Notices of eviction for non-payment of rent, noise violations and other causes, notice of intent to show units to prospective new tenants and other matters are routinely posted on the doors of tenants for all to see who have to walk past that door.

In one landlord-tenant case in which I have worked, one vindictive landlord served notices to show the tenant's unit over a dozen times. He did this by posting a 24-hour notice on the tenant's door and did so for at least 12 days in a row. If memory serves correctly, I think the number is probably closer to 17 days in a row. Not once was there a proper 24-hour notice given nor was there ever any attempt to follow up by actually bringing along prospective tenants.

Subsequent tenant hearings supported the tenant in the case, but what other visitor or tenant walking past that person's door got that side of the story — a very private story that needed not be so publicly displayed? From reading notices posted on other units, I and other tenants in this province become routinely aware of what tenants are being evicted and why.

We form opinions and do so based on only the landlord side of the story, when it's often reversed at hearings. It's one in which we never hear the final outcome, which may well support the tenant.

Ten of Canada's 13 provinces and territories mandate that while postings of this nature meet the requirements of their tenancy laws, the landlord must first justify to authorities why such a public posting is necessary. An example of justification often used is that the tenant tries to avoid document service. In the other

three, no such prequalifier exists. That's the situation today in B.C.

Lazy landlords can and do use this posting as their first means of communications. B.C.'s PIPA says that is not fair. In fact, PIPA makes it illegal. But the provincial Residential Tenancy Act, the RTA, has several sections that say it's not only okay but our provincial government produces various fact sheets telling landlords and tenants how to go about posting if they want to.

The province's small claims court act, the provincial family court act and the Supreme Court Act of this province do not allow such service as a first attempt at communications. So why does the RTA?

[1330]

I believe this oversight is directly linked to the PIPA wording at section 4(1) and the RTA provisions at sections 2(1) and 5(1). PIPA section 4(1) notes that conflicting PIPA provisions override other provincial legislation unless the offending act expressly provides that the other enactment or a provision of it applies despite this act.

At law this verbiage may be correct, but in common language, for the people on the street to understand, I believe this section can be strengthened to eliminate any confusion by replacing the words "this act" with the words "the Personal Information Protection Act." Thus done, an argument that the quoted RTA sections that suggest the act may apply over the provisions of the PIPA would be more obviously without merit.

I have a presentation to hand out, and in that presentation, I have the exact sections of legislation all across town in their 13 jurisdictions for your perusal. In addition, I have the exact quotes of the Residential Tenancy Act with regards to section 2 and section 5 for your perusal.

That, basically, is my presentation. Thank you for your attention.

**R. Cantelon (Chair):** Thank you for your presentation and for taking the time of cross-referencing it for us. That will be useful to the committee.

Do any members of the committee have questions they wish to put forward to Mr. Armstrong?

**L. Krog:** Thank you, Mr. Armstrong. Have you made any representation to the residential tenancy branch about this as well?

**B. Armstrong:** I have not yet, but I may very well do so. I think it would carry some considerable clout if you folks would also make that presentation to them.

**R. Cantelon (Chair):** Thank you again, Mr. Armstrong. Seeing no further questions, I appreciate it. Thank you for providing a written submission, as well, that we can peruse later.

We'd like now to call forward the next presenter. It's an association known as Xtract — Mr. Roger Phillippe.

**R. Phillippe:** First of all, I'd like to compliment the committee for taking the initiative to advertise this

hearing throughout British Columbia. As a direct result of this advertisement, I'm able to provide the opportunity for my submission today.

What I'm going to talk about is the impact of privacy law on property crime prosecution and stolen property recovery.

A little background. The persistent patterns of property crime have resulted in city, municipal and town councils implementing transaction-reporting by-laws regarding secondhand merchants. Property crime in Vancouver is the highest in Canada. Daily reminders in the newspaper are showing troubling national trends, especially in metal theft.

There is invariably a need for accurate personal information in order to investigate crime. The secondhand sector serves as an advance test bed for the balancing act society faces when weighing privacy rights against the needs of both the merchants and the police agencies across Canada.

The city of Vancouver charter presently allows for the collection of personal information at all secondhand stores. It includes pawnshops, scrap metal dealers, music stores, jewellery stores, sports stores, consignment stores and a whole range of other secondhand dealers. This can include stores like London Drugs, who do second-hand, or Birks or Kerrisdale Cameras, who do trade-in of cameras.

In contrast, a recent court of appeal decision in New Westminster resulted in the key component of a bylaw being struck down while it restricts the reporting to police of a customer's personal information. Non-existent and inconsistent bylaws define or leave to the merchant's discretion what personal information is collected. Identity information which may be needed for a valid criminal investigation can no longer be sent.

[1335]

Why is personal information required? First of all, the police are not getting the personal information, and it hobbles an investigation. Because of the ability to link that property to the property, it's removed. For an example, if a crime occurs where several pieces of stolen property are taken by a thief to four different secondhand stores, not all these items are serial-numbered, and without an identity marking linking this suspect, the police cannot find non-serial-numbered property or connect the items to one theft.

Therefore, at least one piece of government photo ID should be produced to positively identify the person who is exchanging goods. This ID should have some type of physical descriptors as well.

I think it would be in the best interests for a national serial number-matching system. A recent cost-effectiveness report for the city of Edmonton showed that during the year 50 percent of the hits from a city-wide electronic reporting system were achieved without the use of private personal information. The simple serial number-matching proved powerful, despite the fact that only an estimated 2 percent of the victims retained serial numbers for the stolen merchandise. Based on Edmonton's population, politicians can easily extrapolate the direct public benefits of local, regional and national systems.

The possible privacy-sensitive solutions. An effective system of verification of personal identification could and should involve the use of photo identification using the registration number from ID. Ultimately, there has to be a compromise between the privacy issues and policing. The privacy wants to give less, and the police want more.

Customer privacy will be maintained in this scenario. The merchant could retain client personal information on his own database in a secure or even encrypted style. Only the numeric information, plus the pawner's name from the photo identification, would have to go forward to the police, along with an effective description of the sold items. Should a police investigation be warranted, accurate personal information linking the suspect to the crime would be available.

At present there is an impending crisis in Ontario. Ottawa, the nation's capital, is now the test case for merchants' rights to collect data. If B.C. follows Ontario's privacy leads, where Ottawa shops can only record bare contact information — which is just the name, the address and a phone number — from the clients, the trend in privacy laws will create more property crime with the ease of getting rid of stolen property.

The city of Ottawa has ordered the shops to destroy all non-bare essential contact information, effective February 28, 2008. I have an attachment. I also have noted a web link on my handout, which I will be passing out.

Proposed consultations in Ontario. Absent in B.C. is the discussion of a consultative process for the development of new bylaws and possible provincial laws. In Ontario the Information and Privacy Commissioner has accepted a request from the Ontario Association of Chiefs of Police for such a dialogue. I also have two attachments for that.

In conclusion, the B.C. Community Charter does not presently address the ability of police or merchants to collect personal data. In this new regulatory context the provincial government must step up to the plate to rectify this deficiency, in the public interest. If property crime is a priority, society needs legislation now and not later. Ultimately, what is required is a provincial secondhand dealers act coordinated with an anti-fencing initiative.

[1340]

Again, I would like to thank the committee for hearing my presentation today. Given the short time frame, I would also like to be provided time to make a further detailed submission. I have tried to collect relevant information from other provinces, but this is a short time frame for me.

**R. Cantelon (Chair):** Thank you very much for your submission. If you do wish to add further to it, please feel free. We are open for written submissions for some time.

Do any of the committee members have questions?

**L. Krog:** Thank you very much, Mr. Phillippe. I take it you work in the industry, so to speak.

**R. Phillippe:** Yes, I work for a company called Xtract. Xtract is software that deals with the pawnshop and secondhand scrap metal reporting to the Vancouver city police as well as RCMP in Chilliwack and Kelowna.

My background is 38 years with the RCMP. I just retired last year — 33 years in forensics.

**L. Krog:** In your experience and based on your work with the police, would you say that there's general support in the policing community for this kind of a proposition?

**R. Phillippe:** Right now from B.C. to Ontario nobody knows what's going on. The Privacy Commissioner in Ontario, Ann Cavoukian, has ordered the destruction of records from the Ottawa city police as of the 28th of February. Basically, in Ontario — it's filtering right across Canada as well — the police are scared to do anything. They're scared to collect information.

What's happening is that the scrap metal dealers, the pawnshops or the secondhand dealers are getting frustrated because they can't do the reporting to the police because the police are not taking their information. Until an act, a provincial law, is passed where this is all sorted out, there's going to be a lot of confusion.

**R. Cantelon (Chair):** As your presentation points out, this may involve other jurisdictions and other acts. We certainly will take the matter under consideration. Where it does or doesn't apply.... I'll see that we forward it to the appropriate ministry for their consideration as well.

The Association of Fundraising Professionals for Vancouver Island. Mandy Parker is present.

Thank you, Ms. Parker. The floor is yours.

**M. Parker:** My name is Mandy Parker, and I'm here today representing the Association of Fundraising Professionals for Vancouver Island. I've provided each of you with the AFP fact sheet for your reference — AFP refers to Association of Fundraising Professionals — along with the AFP *Code of Ethical Principles and Standards of Professional Practice* and the *Donor Bill of Rights*.

Just to give you some background, AFP is the largest community of fundraisers in the world, representing more than 29,500 individuals in over 195 chapters around the world who are responsible for generating philanthropic support for every conceivable charitable cause. AFP works to advance philanthropy and ethical fundraising, and AFP's code of ethical principles and standards of professional practice is the gold standard in the fundraising world and has been used as a model for charities around the world. AFP has nearly 3,000 members and a network of 16 active chapters across Canada.

[1345]

The non-profit sector comprises more than 160,000 organizations, of which approximately 80,000 are registered charities. Together they bring in more than \$100 billion in annual revenue and possess even more in net assets. It's approximately equal in size to the economy of British Columbia.

AFP Vancouver Island has over 100 members. We have an active board of directors with a number of working committees, one of which includes professional standards and ethics. When PIPA came into action, AFP Vancouver Island informed its membership of compliance requirements. The board of directors made themselves available to the members, should they have any questions.

We fully encouraged our membership to become informed about the implications and the compliance. AFP Canada has put together a number of documents which are readily available to anyone who accesses the AFP website, and they were distributed to the membership when they were first developed.

The first document, *An Introduction to Protecting Personal Information Collected by Charities*, was developed by AFP and its privacy task force. The document provides a general overview of the federal PIPEDA Act, including the principles behind the privacy legislation, how the bill works, what constitutes personal information, the complaints process and resources for further information.

The second document prepared by AFP, the Association for Healthcare Philanthropy, the Association of Professional Researchers for Advancement and the Canadian Centre for Philanthropy, is a more in-depth guide to privacy. Titled *Privacy 101: A Guide to Privacy Legislation for Fundraising Professionals*, this manual provides specific strategies, activities, examples and sample documents to help charitable organizations comply with the federal law.

The third document, prepared by the same group as above, titled *Fundraising and Privacy: Complying with Federal and Provincial Laws*, provides the basic principles of the current federal and provincial privacy laws in place as well as tips and guidance for fundraisers and charities for trying to comply with those laws. While these resource materials are strictly for informational purposes and are not legal advice or opinion, they should help Canadian fundraisers and charities understand and fulfil their responsibilities underneath the federal and provincial laws.

AFP Canada does have a government relations committee, in which AFP Vancouver Island participates. We work together to ensure that our members have the most current and up-to-date information. We understand that the committee is currently drafting FAQs to help charities and other non-profit organizations comply with the PIPA legislation.

We would like to extend our services and vast expertise to the Office of the Privacy Commissioner to help with the drafting of this document. AFP has considerable experience in drafting informational materials for regulatory compliance both here in Canada and abroad, so please consult with us and AFP Canada with respect to this issue and any other privacy issues that might affect the charitable sector. We're here, and we're happy to help.

**R. Cantelon (Chair):** Thank you very much for your presentation.

Do any of the members have some questions?

I hear none, but I have one. On the *Donor Bill of Rights*, I wonder if you could explain to me.... Section 9 is to have the opportunities for their names to be deleted from mailing lists that an organization may share.

**M. Parker:** Sorry. Can you repeat that again?

**R. Cantelon (Chair):** On the *Donor Bill of Rights*, on the last page that you handed us.... Section 9 under that is to have the opportunity for their names to be deleted from mailing lists that an organization may intend to share.

**M. Parker:** Correct.

**R. Cantelon (Chair):** How does that work in practice? It's incumbent on the individual to have their name removed from a mailing list or otherwise....

**M. Parker:** What typically happens is that an individual may phone a charity and ask for their name to be removed from the mailing list. What charities typically do is record in a couple of places that that individual.... We work with a database. Typically, fundraisers work with a fundraising database. What charities typically do is mark a "do not mail" on the person's record.

We have to keep the actual record because of the gifts that they have made, and they have to be kept because of the charitable tax receipt numbers that were there. But they can mark "do not mail" and then delete their address information. Then it's recorded when the person called and asked that they be removed from the mailing list.

[1350]

**R. Cantelon (Chair):** My concern goes to the fact that unless they take an active role in having their name removed, it can be sold, rented or exchanged with other organizations. It's incumbent on the individual to make sure that their information — which certainly, I presume, beside their name might include their address and contact information — can be shared unless they're alerted to the fact that they have to take it off.

**M. Parker:** Most of the charities — certainly the charities that are involved with the Association of Fundraising Professionals — have a disclaimer on all of their solicitation materials indicating what the information is used and collected for. Typically, organizations will mark down that the lists are not for sale.

Certainly, the organization that I work for and a lot that I work with.... We do not sell our donor lists.

**R. Cantelon (Chair):** I see no questions, so once again, thank you for coming and making this presentation.

I believe that the United Auto Trades Association of British Columbia has arrived.

Thank you for coming, Mr. Hancock and Mr. Preddy. Please come forward and make your presentation.

**G. Hancock:** Good day, and thank you for having us this afternoon. I'm George Hancock, past president of the United Auto Trades Association, and I have with me Gerry Preddy, who is the vice-president of the Auto Trades Association.

What we want to do today is present a real-life example of what it is like for associations and private citizens to put a complaint into the privacy commission.

As we say in our handout, we'd like to thank everyone for going the extra mile in doing what we're doing here. We appreciate the ability to participate in the democratic process that we have here today. We hope that we will do more of these in the future.

The United Auto Trades Association is comprised of auto repair and auto glass repair shops. The UATA has a complaint registered with the Office of the Information and Privacy Commissioner for B.C., and that complaint remains unresolved. Our file number is F0526563, and the complaint was initiated in June of 2005.

Our complaint revolves around a Crown corporation that is contractually forcing repair shops to collect and hand over customers' sensitive financial information. The employees of the corporation then take the information off-site for evaluation for up to 30 days.

The repair shops have a contractual obligation with credit card companies. One such agreement states: "A merchant must not sell, purchase, exchange or in any manner disclose MasterCard account number information to anyone other than its acquirer, to the MasterCard Corporation or in response to a court order request. This prohibition applies to card imprints, transaction receipts, carbon copies, mailing lists, tapes and other media obtained as a result of a MasterCard transaction."

Clearly, furnishing credit card information to anyone without a court order will leave a vendor subject to prosecution. Our vendors feel completely powerless when faced with the dilemma they are put in as a result of a rogue corporation operating with no accountability.

The Crown corporation in question claims that in order to reduce fraud and to ensure customers are paying deductibles, it is necessary to audit retailers' accounts. Audits are conducted as a result of a premonition or unsubstantiated complaints, which appears to be the established practice. We would contest that this reason should not override the rights of the public nor cause repair shops to be in non-compliance with credit card agreements.

[1355]

This raises some questions. Why would a Crown corporation continue with programs that conflict with the lenders' agreements, and why is the corporation so unresponsive in light of the OIPC's continued questioning?

We also contend that the corporation may have other reasons for wanting to take documents off-premises. This is especially the case when there are other simple solutions that would entirely eliminate the non-collection of deductibles and associated fraud. The solution is entirely within the corporation's ability to enact. In fact, they have previously mentioned the possibility of collecting deductibles themselves.

We note in the letter to the OIPC from the Trial Lawyers Association of B.C. that the trial lawyers consider the Insurance Corporation of B.C. to be in an inherent conflict of interest with the monopolistic insurer in B.C. ICBC, in response, deny that they store information taken off-site.

In closing, we trust it is abundantly clear that the Insurance Corporation of B.C. remains unfazed, despite scrutiny by the OIPC, the Trial Lawyers Association of B.C., the UATA, and other groups for that matter. It is unfortunately also clear that ICBC is actively involved in reducing the effectiveness of the Privacy Act. Therefore, we firmly believe that the OIPC must be above influence by Crown corporations to be effective.

The complaint brought forward by the UATA is nearing its three-year mark. The UATA believes that the reason for delay in obtaining a ruling on this issue is partly due to stonewalling by the corporation but, more importantly, is due to a lack of funding experienced by the OIPC. It is our belief that the OIPC performs a service that protects our privacy and that no price is too high. We hope to convince our government to fund the OIPC appropriately and to keep the OIPC at arm's length from government corporations.

On behalf of the UATA, I thank you for the opportunity to present our views.

**R. Cantelon (Chair):** Thank you very much.

**L. Krog:** I'm just wondering if you could give us a concrete example of what you're talking about in practice.

**G. Preddy:** In practice, an employee of the corporation will go into a repair facility and gather a file. Within the file is sensitive information such as credit card numbers, addresses, phone numbers — everything to do with that particular customer — and it's taken off-site.

Our concern is that they are taken off-site with no control whatsoever. They could be left in their trunk. They're collecting this from many shops at one time, and it's done ad hoc. It's not systematically done so that they know that they're coming. Our problem with this is that the information taken off-site has not been authorized by the people who own that information, which is the public themselves.

We have examples of complete bank statements being taken off-site. There are a couple of examples of missing documents that didn't come back. There are examples of documents having been taken off-site, and they've said: "Well, you've got a copy of it, so we'll just keep this copy." So we know that they're taking it off-site and keeping it. Our concern is that this sensitive information is open for abuse, and we believe that it is unnecessary for them to do so.

**L. Krog:** If I may, with the Chair's indulgence. You mentioned a bank.... Why would a member of your association have a bank statement for a customer?

**G. Preddy:** Not bank statement, a cancelled cheque with cheque number. Sorry. Thank you for the correction.

**L. Krog:** So I've come in to get my windshield repaired, and I pay my deductible. The purpose of ICBC collecting this information is to ensure the deductible is in fact paid. Or are they concerned about fraudulent claims and involving the provider of the services, which is presumably a member of your association, or exactly what is it they're getting at? Why do they need this? What's the explanation?

**G. Preddy:** The main explanation is the collection of deductibles. We don't have a problem with that. However, we believe there's a much simpler method of collecting the deductibles that will not interfere with the Privacy Commissioner.

We believe that the information they take off-site is where the real problem is. Individuals' information should not be, and it's illegal for them to take it. They're breaking the law every time they take a file with private information off-site. It's very clear that that information is to be kept between the repairer and the owner of that vehicle — period.

[1400]

**G. Hancock:** If I may. The simple fact that the file is two and a half years old would tell me that our privacy laws aren't working, because there is no question that what ICBC is doing is breaking the law. We've had the trial lawyers look at it, and their reasoning is that yes, they are absolutely breaking the law. They've written a letter to the commissioner asking the commissioner to enforce the laws.

That's our main problem — not what ICBC is doing, but the lack of response in getting them to stop doing what they're doing.

**L. Krog:** The fact that I've been on holiday for two weeks may reflect on me being terribly obtuse about this. Again, if I come into your shop, I hire your services to repair my windshield or replace it, and I have a \$200 deductible, you're going to want to collect the \$200 from me. You're in business. If you don't get it from me, you don't get to collect it from ICBC.

**G. Hancock:** Right, absolutely.

**L. Krog:** So why does ICBC require the records in order to ensure that the deductible has been paid? What am I missing?

**G. Preddy:** Absolutely. Thank you for bringing that up, because in fact it is the portion of the insurance claim that the Insurance Corporation has no financial interest in whatsoever. It is confusing as to why they're so interested in that collection of the deductible.

It is fraudulent for the insured to not pay that deductible. We know that through the Insurance Act. It is confusing, because it could simply be answered by the Insurance Corporation collecting the deductible at the

beginning. Then we wouldn't have this situation, and that would end it all. It's a very simple fix. Our concern is not so much with the corporation but with the lack of movement from the Privacy Commissioner to enact the law, to ensure that this type of exchange of information can't take place. We would like that to stop.

**L. Krog:** I take it that, essentially, this is aimed not so much at individuals but at members of your association who ICBC believes are engaged in some sort of fraudulent activity — in other words, a shop that's really just a place where everyone goes in, pretends to put a windshield in and charges ICBC above and beyond the deductible. Is that what it's aimed at — that kind of fraudulent practice?

**G. Hancock:** No. We believe that ICBC.... Really, that kind of fraud is almost impossible to do now, because in order for vendors to get paid, they first have to have the file in ICBC's main computer. So it's almost impossible to do that kind of fraud.

The kind of fraud that ICBC is mentioning is the non-collection of deductibles. I guess it is fraud, but as you say, if the vendor doesn't collect the \$200 deductible, he's out the \$200. We do not want our members or anyone to waive deductibles, because it's just plain bad business. We think the reason that ICBC is not collecting the deductibles themselves and that they're going after these repair shops is that basically, they're getting information. We think they possibly are profiling, so that they can.... That's what every insurance company in North America wants to do, of course: to profile us.

There's a good example of that in the last few days. If you had the wrong postal code, you're going to pay more money for your insurance. We know for sure that they're doing that sort of thing, and we think that's why they're wanting to get the records from the repair shops.

**R. Cantelon:** If I may, Mr. Krog, I think they're suspecting, perhaps, collusion between the two — that the deductible is never collected and that there's an inflated price. This is a way to check that, but certainly Mr. Krog and I and the Deputy Chair will take an interest in pursuing why this has not been moved forward, and we'll obtain the reasons why. I thank you for your submission.

**G. Preddy:** Just like to correct this. Although I'm honoured to be named after Penny Priddy, my name is spelled with an "e", not an "i."

**R. Cantelon (Chair):** We apologize for that, and I'm sure Penny Priddy is also in agreement.

[1405]

Now is Laura Knight here, the representative from the Insurance Brokers Association of British Columbia? If she is, I'd ask Laura to come forward and make her presentation.

Miss Knight, the floor is yours.

**L. Knight:** The insurance brokers are major collectors and keepers of personal information. B.C.'s property and casualty insurance brokers handle more than four million face-to-face transactions with consumers per year, and that's just for auto insurance.

The vast majority of all insurance policies for homes, vehicles and businesses written in the province are handled by insurance brokers — and more specifically by brokers who are members of the Insurance Brokers Association of B.C. These insurance transactions are conducted mostly in a small business environment.

Insurance brokers were required to comply with the federal Personal Information Protection and Electronic Documents Act — PIPEDA — on January 1, 2004, along with other private sector businesses. The transition was relatively smooth, and as far as we know, the compliance performance of brokers has been excellent. This was due to privacy practices that were already in place for the insurance brokerage industry, as brokers were already compliant with the Freedom of Information and Protection of Privacy Amendment Act, which establishes privacy requirements for government ministries, agencies and Crown corporations such as ICBC. Also, preparation by the Insurance Brokers Associations of B.C. and Canada, which provided training and sample forms for member brokers starting about two years prior to the compliance date.

The Insurance Brokers Association of B.C. was pleased to be consulted prior to the drafting of the Personal Information Protection Act. We were able to make a couple of suggestions for minor language changes to assist in the unique aspects of insurance and the principal agent relationship. That was 8(2)(a) and (b), which deem that consent has been given by parties with a minor interest in an insurance policy, thus allowing coverage to proceed on the authority of the party with the major interest; and 12(2)(a) and (b), which provide for the role of the agent in the collection and use of personal information.

We'd like to report that these clauses are working well for the insurance industry, and the drafters of the PIPA should be proud that some stakeholder submissions to the federal PIPEDA review have recommended that these clauses be incorporated into the PIPEDA.

The PIPA allows verbal consent, which is helpful for the insurance industry and should be continued. When consumers ask for an insurance quotation, brokers explain that certain personal information must be collected because the insurance policy and premium is based on the value of the assets being covered. Consumers, therefore, can choose to divulge the information or not.

For a consumer to have to provide written consent prior to freely giving such information would be redundant and unnecessary. Provincial legislation must be substantially similar to the federal PIPEDA. So we appreciate the changes to the PIPA must be made within those substantially similar parameters, and that may limit the extent to which our recommendations can be acted upon in B.C.

First would be blanket consent. The federal Bank Act and the provincial Financial Institutions Act both provide for insurance as a financial pillar that's sepa-

rate and distinct from other banking functions. This provides protections and safeguards to allow consumers to purchase adequate and appropriate coverage for their important assets in an environment free from inducements, obfuscation or coercion.

In real terms, the statutes dictate that insurance can only be sold and insurance advice can only be given by qualified, licensed personnel. Banks can own an insurance subsidiary but are prohibited from retailing insurance from their branches. The business office of the insurance agent must be located in premises that are separate and distinct from the business office of a savings institution.

IBABC member brokers are extremely concerned that we're seeing blanket consent forms used by banks that include language that grants them permission to share personal information across the banking and insurance pillars. In our view this is contrary to the intent of the federal Bank Act and the provincial Financial Institutions Act.

We were pleased to see, in the proceedings of this committee's meeting on May 29, 2007, that the issues of identity theft and misuse of credit information were addressed. We're also concerned that blanket consent forms can be used to gain permission to use credit information in ways that the consumers may not be aware of, and if the consumers were made fully aware, would not agree to.

[1410]

In our view, there is an opportunity for the PIPA to be in alignment with and to strengthen provisions of part 6, "Credit Reporting," of the Business Practices and Consumer Protection Act. It provides for sharing of credit information as long as the individual gives permission, and it requires that organizations using the information to disclose the reasons for adverse actions, such as denial of sale or increase of cost, that may result from the use of that information.

We urge the committee to include a clause in the PIPA that prohibits blanket consent across financial pillars and to review the relevant sections of the PIPA in conjunction with part 6, "Credit Reporting," of the Business Practices and Consumer Protection Act.

A little bit about IBABC. The Insurance Brokers Association of B.C. serves as the voice of the general insurance brokerage industry and promotes its members as the premier distributors of insurance products and services in British Columbia. IBABC is the primary provider of prelicensing and continuing professional education for the general insurance brokers in B.C. IBABC represents the interests of the public and its member brokers to government and to industry stakeholders.

IBABC represents about 750 property and casualty insurance brokerages that in turn employ more than 8,000 people in approximately 140 B.C. communities. Member offices are the consumers' choice for the vast majority of all property and casualty insurance policies and premiums written in the province.

Consumer satisfaction with their insurance brokers is high. In survey after survey, consumers report that they value their insurance broker's knowledge, profes-

sional advice, unbiased review of their needs and coverage options, and service and advocacy in the event of a claim.

IBABC member brokerages have an average of 13 staff members and, therefore, fit within the small-to-medium-sized-enterprise category.

**R. Cantelon (Chair):** Thank you very much.

**M. Polak:** With respect to your recommendations, are these issues which are new, which are something that you're seeing recently? I'm curious as to why it wouldn't have been captured in the initial consultations around the act.

**L. Knight:** I think the issues that we're seeing are becoming more and more obvious to us.

**L. Krog:** I take it that people who work in the industry are finding that banks are making requests for information that historically weren't happening. Is that fair to say?

**L. Knight:** I think that would be fair to say, and perhaps it's worded in such a way that it doesn't allow the consumer to realize exactly what they're signing on to.

**L. Krog:** So the consent forms as you describe them are blanket. Most people going into a bank and asking for a loan expect to have credit information released. That would be, I think, their expectation.

**L. Knight:** Probably, yeah.

**L. Krog:** What you're saying is that in fact it's now being used to make inquiries with insurance companies. That would obviously include, I presume, life insurance companies as well?

**L. Knight:** I'm not sure about the life insurance companies, but I believe that would be accurate.

**R. Cantelon (Chair):** Well, thank you for raising these concerns and putting forth these suggestions. The committee will certainly take them into serious consideration. Thank you for appearing today.

**L. Knight:** Thank you. If there's anything that we can do to help, just let us know.

**R. Cantelon (Chair):** We will.

That concludes the list of scheduled presenters today. Is there anyone in the audience who wishes to come forward and make a presentation?

We will then take a recess until three o'clock and see if anyone else has appeared. At that time we will reconvene and consider whether or not we need to carry on for the full allotted time, if that's in agreement with the members. Okay?

**J. Rustad:** Okay, good. I'll call back in at three, then.

**R. Cantelon (Chair):** Okay, John. Thank you. The committee is recessed.

The committee recessed from 2:14 p.m. to 3 p.m.

[R. Cantelon in the chair.]

**R. Cantelon (Chair):** I'd like to call the committee hearing back to order for the PIPA committee. The time is now past three o'clock, and during the recess no one has appeared. I would submit that we can conclude the meeting today. It doesn't appear that anybody else will arrive.

**L. Krog:** One item, Mr. Chair. I believe that a reflection of my lengthy absence in a warmer climate may have accounted for the fact that I introduced myself as the vice-Chair of this committee, which I'm not. I wish to ensure that the record is corrected, then.

**R. Cantelon (Chair):** Thank you. Your aspirations are duly noted as well.

#### Next Committee Meeting

**R. Cantelon (Chair):** Now, we have had several presentations on the matter from Vancouver, so it would seem that we will need, indeed, another six presentations.

**K. Ryan-Lloyd (Clerk Assistant and Committee Clerk):** That's correct. Six individuals have expressed interest in appearing before you in the Vancouver area, should a date be identified for that.

**R. Cantelon (Chair):** Such as February 28.

**K. Ryan-Lloyd (Committee Clerk):** We propose, for your consideration, a Friday in Vancouver, given that the House is now back in session, so possibly the 22nd of February or the 29th.

**R. Cantelon (Chair):** Right. The 29th. We have the 29th. I was going to say the 28th.

How does that sit with the members here?

**M. Polak:** If it has to be the 29th, I can accommodate it, but I would prefer that it was the 22nd.

**R. Cantelon (Chair):** Mr. Lali, we've had a number of submissions from people who wish to present in Vancouver. We're looking at the date of the 22nd. That's Friday. I presume it would be something probably not longer than we did today — a couple of hours.

**H. Lali (Deputy Chair):** I don't think that should be a problem.

**J. Rustad:** The 29th I will not be available. The 22nd I may also not be available in person, but I might be able to attend by phone.

**R. Cantelon (Chair):** Does the 22nd sound good?  
We'll say one o'clock at this time.  
Would you prefer morning or afternoon?

**J. Rustad:** My preference would be morning.

**M. Polak:** Mine as well.

**L. Krog:** Yes.

**R. Cantelon (Chair):** Right. At 9:30 or ten o'clock,  
depending on how many we have.

**H. Lali (Deputy Chair):** My preference probably  
would have been the afternoon.

**R. Cantelon (Chair):** You're outvoted.

**H. Lali (Deputy Chair):** I probably am, but let me  
see. Yeah, what the heck.

**R. Cantelon (Chair):** Okay. Very good.  
Motion to adjourn. The meeting stands adjourned.

The committee adjourned at 3:03 p.m.

## HANSARD SERVICES

Director  
Jo-Anne Kern

Manager of Print Production  
Robert Sutherland

Post-Production Team Leader  
Christine Fedoruk

Editorial Team Leaders  
Laurel Bernard, Janet Brazier, Robyn Swanson

Senior Editor — Galleys  
Heather Bright

Technical Operations Officers  
Pamela Holmes, Emily Jacques, Dan Kerr

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

Researchers  
Mike Beninger, Caitlin Roberts, Pavlina Vagnerova

Editors  
Catherine Cardiff, Aaron Ellingsen, Margaret Gracie,  
Jane Grainger, Linda Guy, Barb Horricks, Bill Hrick,  
Paula Lee, Nicole Lindsay, Donna McCloskey,  
Cristy McLennan, Constance Maskery, Jill Milkert,  
Lind Miller, Lou Mitchell, Karol Morris,  
Dorothy Pearson Erik Pedersen, Janet Pink,  
Melanie Platz, 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](http://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.