



4th Session, 37th Parliament

---

REPORT OF PROCEEDINGS  
(HANSARD)

---

SPECIAL COMMITTEE TO REVIEW THE  
**FREEDOM OF INFORMATION  
AND PROTECTION OF PRIVACY ACT**

Victoria

Wednesday, January 28, 2004

Issue No. 7

BLAIR LEKSTROM, MLA, CHAIR

ISSN 1708-315X

Published under the authority of the Speaker

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

[www.leg.bc.ca/cmt](http://www.leg.bc.ca/cmt)

**SPECIAL COMMITTEE TO REVIEW THE  
FREEDOM OF INFORMATION AND  
PROTECTION OF PRIVACY ACT**

Victoria  
Wednesday, January 28, 2004

*Chair:* \* Blair Lekstrom (Peace River South L)

*Deputy Chair:* \* Mike Hunter (Nanaimo L)

*Members:* Bill Belsey (North Coast L)  
\* Harry Bloy (Burquitlam L)  
\* Jeff Bray (Victoria-Beacon Hill L)  
Hon. Tom Christensen (Okanagan-Vernon L)  
Ken Johnston (Vancouver-Fraserview L)  
\* Harold Long (Powell River-Sunshine Coast L)  
\* Sheila Orr (Victoria-Hillside L)  
\* Barry Penner (Chilliwack-Kent L)  
Gillian Trumper (Alberni-Qualicum L)  
John Wilson (Cariboo North L)  
\* Joy MacPhail (Vancouver-Hastings NDP)

\* *indicates member present*

*Clerk:* Kate Ryan-Lloyd

*Committee Staff:* Josie Schofield (Committee Research Analyst)  
Mary Walter (Committee Researcher)

---

*Witnesses:* Dr. Colin Bennett (University of Victoria)  
Dr. David Flaherty  
Ted Hayes  
Tamara Hunter



## CONTENTS

Special Committee to Review the  
Freedom of Information and Protection of Privacy Act

Wednesday, January 28, 2004

	<b>Page</b>
Presentations .....	125
T. Hunter	
D. Flaherty	
C. Bennett	
T. Hayes	
Other Business.....	147



## MINUTES

# SPECIAL COMMITTEE TO REVIEW THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT



Wednesday, January 28, 2004  
11 a.m.  
Douglas Fir Committee Room  
Parliament Buildings, Victoria

**Present:** Blair Lekstrom, MLA (Chair); Mike Hunter, MLA (Deputy Chair); Harry Bloy, MLA; Jeff Bray, MLA; Joy MacPhail, MLA; Harold Long, MLA; Sheila Orr, MLA; Barry Penner, MLA

**Unavoidably Absent:** Bill Belsey, MLA; Hon. Tom Christensen, MLA; Ken Johnston, MLA; Gillian Trumper, MLA; Dr. John Wilson, MLA

1. The Chair called the meeting to order at 11:02 a.m.
2. The following witnesses appeared before the Committee and answered questions:
  - Tamara Hunter
  - Dr. David Flaherty
  - Dr. Colin Bennett
  - Ted Hayes
3. The Committee discussed the invitation of additional witnesses with respect to issues raised in a recent academic report and a *Toronto Star* news article series.
4. In response to requests, the Committee agreed to make public the written submissions once they have been received and reviewed by Committee Members.
5. The Committee adjourned at 1:34 p.m. to the call of the Chair.

---

Blair Lekstrom, MLA  
Chair

Kate Ryan-Lloyd  
Clerk Assistant and  
Committee Clerk





WEDNESDAY, JANUARY 28, 2004

The committee met at 11:02 a.m.

[B. Lekstrom in the chair.]

**B. Lekstrom (Chair):** Well, good morning, everyone. I would like at this time to call the Special Committee to Review the Freedom of Information and Protection of Privacy Act to order and to welcome everyone here this morning. Today we will hear from some witnesses on their views on how the act is working — views that they feel could improve how this act works for the people of British Columbia. My name is Blair Lekstrom. I am the MLA for Peace River South and have the privilege of chairing this committee, which is a committee of the Legislative Assembly.

With that, we do have an agenda today that I think we are going to be pressed to get through. I think the information is going to be valuable. We will start with our first presentation this morning. Tamara Hunter, who is with us, is with the B.C. branch of the Canadian Bar Association. Good morning and welcome, Tamara.

#### Presentations

**T. Hunter:** Good morning. Thanks for the opportunity to speak to you.

The first point I want to make is that you should have some written submissions with three tabs that say Davis and Co. on the front of them. You might want to follow that when I'm speaking. I'm going to start on page 3. The numbering is in the bottom right corner.

Before I get started, just a point of clarification. I am the co-chair of the freedom of information and privacy section of the B.C. branch of the Canadian Bar Association. But when I'm making my comments today, I'm here with a different hat on, which is as a lawyer who practises in the area of freedom-of-information and privacy law. So the comments I'm giving you are my own personal views gathered from that experience. I'm not meaning to represent the views of the association.

We actually have a very diverse section membership. They have very different views about this sort of thing, depending on how they practise and where they're coming from, so it's quite hard for us to come to a consensus view. We've asked our members to send their comments to you directly or to ask to speak to the committee so that you'll get as good a range as you can. I guess what I'm telling you is that there is no consensus view of our section. I'm just giving you my own views as a practitioner.

I was asked to comment on the strengths and weaknesses. The first point I want to make is that I think the act has far more strengths than weaknesses. Generally speaking, from a practising lawyer's point of view, I think it's working fairly well. I do have a few specific comments, but the overall picture from my

point of view is that it works quite well, and it's fairly balanced legislation.

[1105]

The commissioner's office also, in my opinion, functions quite well. I find them to be very fair and balanced. I find that their mediation process works very well, and we're often able to come up with mediated resolutions where there is a dispute between parties.

The one thing I have noticed, and I set it out at the bottom of page 3, is that over years — and I think this is due to budgetary constraints — I have found that cases are not moving as quickly through that office as they did in the past. It seems like the portfolio officers have a fairly large caseload to work with, and so there's sometimes some delay in moving things through. That can be frustrating from the point of view of clients I'm acting for and, I'm sure, for the parties on the other side of the matter, as well, and for the portfolio officers. To the extent that your committee has an opportunity to do so, you might consider suggesting a review of the budget of the commissioner's office.

There are a few areas I wanted to bring to your attention that you might want to consider for potential FOIPPA amendment. They start on page 4. There are three areas I wanted to talk about. The first one has to do with the exception to disclosure where it would be harmful to the business interests of a third party. The second area has to do with the exception to disclosure which relates to protecting solicitor-client privileged information — in other words, communications between lawyer and client. The third point relates to the wording of the FOIPPA regulations — in particular, the regulation that sets out who can act for another person when exercising rights available to individuals under FOIPPA.

Going back to the first point, this has to do with the exception to disclosure relating to the business interests of a third party. This exception comes up under section 21 of FOIPPA. I've put some excerpts in at tab A if you wanted to look at them in any detail. What I wanted to bring to the committee's attention — which you may already know — is that the interpretation that's been given to section 21 means that practically speaking, a contract between government and a business, or government and some other third-party organization, is generally accessible. This exception is extremely hard to apply successfully in a scenario where we're talking about a contract or a term of a contract.

Now, section 21 provides a three-part test that a party must meet if it's resisting disclosure of a document under this section. The first part essentially requires that the information has to come within a certain kind of category. In other words, it must reveal trade secrets. It must be commercial or financial information, scientific or technical information, etc. The categorization is the first part of the test. That's usually not an issue. The second part of the test requires that the information was supplied implicitly or explicitly in confidence.

The third part has to do with whether disclosure would be expected to cause a certain type and level of

harm. There are a number of provisions there. For example, the third party would have to show that it would cause significant harm to their competitive position or their negotiating position, or that it would cause undue financial loss or gain to some third party. Again, a business, for example, that has negotiated a contract with government.... Where there's an access request for that document, if the business is concerned that it would hurt its economic interests if it were disclosed, they've got to meet this three-part test, and they've got to meet all three parts of it.

[1110]

Now, in interpreting that section, the commissioner and the courts have interpreted the second part — the part that says "supplied implicitly or explicitly in confidence" — such that it virtually never applies to a contract. That's because the commissioner and the courts have said that "supplied by" doesn't.... When you have a negotiated term in a contract, it's not supplied by one party to another party. It's the result of give-and-take in negotiation. Therefore, it just sort of doesn't even fit that criterion. Even if the business could show that release of that contract or that provision in a contract would harm their economic interests significantly, they will not be successful in defending disclosure or preventing disclosure under section 21.

Now, the committee may already be aware of that, but I wanted to raise it to your attention. It may be deliberate. The committee may look at that and say: "That's appropriate." But I know that businesses consider it undesirable and unfair that where they can show their economic interests would be significantly harmed by release, they're nonetheless out of luck and that document is released virtually all of the time. There are a few exceptions, but they are very specific and difficult to meet.

I think from the public bodies' point of view.... We're not just talking about traditional government public bodies here. Of course, it also would include a professional college, a university, a hospital, a municipality — those kinds of bodies. From their point of view, it can be detrimental to their interests, as well, when they are negotiating with a business to come up with a contract.

One issue is that when contracts are public and the parties know that's going to be the case, it can impact on what the terms of the contract are. It may be that certain businesses are prepared to enter into certain terms with government if they're going to be disclosed, and perhaps in some cases more favourable or different terms, if they know that it will be kept confidential.

That's one issue. I think that's not the most significant issue. The more significant issue — and I'm dealing with this at the top of page 6 — is that in some instances there are going to be businesses or organizations who are simply unwilling to enter into a contract or certain type of contract with government if they have to accept the fact that it's going to be made publicly available. I just gave one example where government wants to be one of a number of participants in a

multiparty contract. Let's say a public body is looking to invest some surplus funds and there's a private investment fund offering an opportunity. The government is one player in that situation. They may not be the majority player. They may be a fairly small player in that situation, and the private sector body may say: "Look. If this is going to mean that the whole deal is made public, we just prefer to leave government out of it." That may not be the result that government wants, and I'd ask you to consider that in the current time frame where government is looking at private involvement in public initiatives or public-private partnerships, this is an issue that needs to be considered.

This is what I'm hearing from my own practice scenario. I'd suggest that the committee might want to try to hear from public bodies on the point and ask them whether this is having a significant impact in terms of what deals they're able to make or not able to make or how much of a factor it is in the deal-making process, because I think from this committee's point of view, that's probably the more pertinent question. I just raise it as an issue.

If the provision is not amended and it's just sort of status quo, what it essentially means is that under FOIPPA, there's always a balancing between the public's right to know other people's individual privacy interests and legitimate third-party interests. With the status quo, essentially, the public's right to know when it comes to a government contract is pretty much absolute. That might be the way the government decides it should be, but you should just be aware that is the case, and it's not necessarily apparent from a reading of section 21. It comes from a combination of the wording and the way it has been interpreted. That's the first point I wanted to make for an area of possible amendment.

[1115]

The second one relates to the issue of the exception to disclosure to protect solicitor-client privileged information. I was involved in a case last year where there was an application that was made to the Legal Services Society for information that, if revealed, could reveal solicitor-client privileged information regarding which clients were receiving legal aid. I was involved with this case from the point of view of the Canadian Bar Association, which felt that it should be protected from disclosure or at least that the third party whose solicitor-client privilege it was should have an opportunity to make submissions and have those taken into account.

In the course of doing that case, it became apparent to us that section 14 — given the way it's worded — has, it seems, been drafted with the idea in mind that when there's an issue of solicitor-client privilege, it will be the privilege of the government body that's at stake. In other words, it will be legal advice that was given to the public body, to government, to the hospital or to whoever the public body is.

It's worded in such a way that it says they may refuse disclosure on the basis that the information is sub-

ject to privilege. That makes sense when it's the government's privilege, because a person can always waive their privilege if they think it's appropriate to do that. But the problem is that if it's someone else's privilege, they shouldn't be waiving it. I mean, it should be something that the person speaks to, and the public body should be protecting it.

The case I was involved in went to the B.C. Court of Appeal. They held that solicitor-client privilege has now been elevated by the Supreme Court of Canada to have a constitutional level of protection, and so the court essentially read in that protection to FOIPPA, despite the fact that it doesn't appear to be there on the face of section 14. What I'm suggesting is that this committee consider an amendment to FOIPPA that would make section 14 and section 22, which I'll get to, consistent with the decision in the B.C. Court of Appeal case.

I think the amendment that would be required is that section 14 state that the head of a public body must refuse to disclose to an applicant information that, if revealed, could interfere with a third party's solicitor-client privilege, but may refuse to disclose information that's subject to the public body's solicitor-client privilege. I set that out in the middle of page 7.

I think the other amendment that would fit with that same idea is one under section 22. Section 22 of the act is the one that protects personal information of third parties. Section 22(3) sets out circumstances where disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy. So that provides a guide and a sort of way for public body heads to decide when to disclose and when not to disclose under section 22.

My suggestion is that the committee consider amending not only section 14 but also section 22 so that it would state that the disclosure of personal information, which if revealed would interfere with a third party's solicitor-client privilege, is presumed to be an unreasonable invasion of the third party's privacy. I think what I'm suggesting is just what follows from the B.C. Court of Appeal case, but I'm sure you have legislative counsel that can help you with that if you're wanting to look at it more closely.

The third area I wanted to suggest to you for consideration for amendment is the FOIPPA regulations, and I did set those out at tab B if you're wanting to look at them. Section 3 of the regulations sets out the circumstances where one person can act on behalf of another person in exercising their rights under FOIPPA — so where they can access records, where they can ask for correction of records or where they could give consent to disclosure.

It deals with a number of instances. It deals with minors, for example, with deceased persons or where the person has a committee appointed. It appears that there are situations that arise that aren't covered in the regulations. One that comes to mind is where a person has been granted power of attorney. The other one that comes to mind is where a person has appointed a representative under a representation agreement.

This, I have to say, is not my own area of expertise, but I sort of came across it tangentially in something I was working on. I'd suggest that the committee might want to seek some guidance from maybe the public trustee's office or a lawyer who works in the area of trust and estates, who could probably delineate for you where else that scenario might arise, because it's a lot simpler for the public bodies if they have the scenarios set out and know what to do in those situations.

Those are the submissions I had. I'd be happy to answer any questions the committee might have.

[1120]

**B. Lekstrom (Chair):** Thank you very much, Tamara. I think you've presented a very good brief to our committee this morning. I'm going to look to members of the committee for questions, and I will begin with Jeff.

**J. Bray:** Thank you, Tamara, for the presentation. Just a question back to your first point about economic interests and third party, because we do hear that a lot. By and large, government tenders are a public process, you know, and B.C. bids on line. Obviously, during negotiations there are sensitive issues and commercial interests, etc., and I understand that. But once my company has agreed to pave a road in Victoria and I'm receiving funds from that public body — the Ministry of Transportation, for instance — could you describe what potential economic threat that contract poses if it were public? If it's just my company paving a stretch of road on Douglas Street, what potential economic interests could be impacted by disclosure?

**T. Hunter:** I think in that particular scenario, which is sort of the more traditional model where you're talking about a business providing a contract to provide widgets or a service, as you say, to government.... The only potential there — and I've just heard this from business clients — is that they may be willing to offer certain terms to government that are favourable to government if it's not public. If it is public, then all their competitors are going to know what that is and all the other parties that are their potential clients know what they've given to government in that scenario, so it impacts on their ability to offer different terms to somebody else. I think that's really the issue.

**J. Bray:** If I could follow up, then the issue really is that normally I'd charge \$4,000 a kilometre. Boy, if I get this great contract with the ministry and it's a lot of work, I'm going to do it for \$3,600, but I don't want everyone else to know I'm giving the cut deal. Is that essentially what you're saying?

**T. Hunter:** That's what I've heard in that scenario. That's why I said that particular point to me is not the biggest issue here for the committee to consider. The bigger point is the less traditional model of contract where it's not the government with lots of economic

clout and purchasing power and one party supplying widgets. It's a multiparty agreement where government is a smaller player and there are a lot of other public bodies involved, maybe different commercial parties involved.

In the scenario you gave, one answer might be: "Well, too bad. Those are the terms of doing business with government. Take it or leave it." There are lots of people who want to supply widgets to government, and it's not a big issue for government. But in the second scenario, sometimes the government isn't the one necessarily with all the clout in the situation, and they may really want the public-private arrangement to go ahead. Sometimes the public nature of the concluded contract can be a factor for the commercial parties in deciding whether they want to participate.

**J. Bray:** My final question: is it your suggestion, under that exception provision, that the three-part test be disengaged?

**T. Hunter:** I'm glad you asked that, because I don't know if I was all that clear about that point. What I'm suggesting is that the first and third parts of the test are probably sufficient to cover the situation. What that would say is where it's in the category of sort of commercial-financial type of information and where you can show that it would be significantly harmful to your economic interests or your negotiating position, etc., then whether it's a contract or whether it's not, it'll be protected. Actually, that third part of the test is not all that easy to me. The commissioner has been pretty exacting about what kinds of evidence he requires to show that. It can't just be fanciful; it has to be shown.

What I'm suggesting is that one alternative for the committee to consider is saying that it being a contract shouldn't completely disqualify it from protection under section 21 and that you should look at the harm that would be caused. Then you'd be balancing the public's right to know versus the economic harm caused, instead of saying: "It's a contract. Forget it. It's not going to be protected."

**J. Bray:** Okay. Thank you.

**B. Lekstrom (Chair):** I'll look to other members of the committee.

[1125]

**J. MacPhail:** Thank you very much, Ms. Hunter. A very good presentation, very thoughtful. Ms. Hunter's suggestion that perhaps we talk to a group like Partnerships B.C. to see how that affects them.... That might be a useful discussion we have with them.

Last week Darrell Evans and his group presented to us about an amendment they were proposing to clarify the exemptions being applied by the courts, I think it is, to expert opinions.

**T. Hunter:** Yes. I know the issue.

**J. MacPhail:** Yes. Do you have a view on that? Does the Canadian Bar Association have a view on that?

**T. Hunter:** The Canadian Bar Association doesn't have a view on that because, quite frankly, our sections never got together and talked about it. I can't tell you what the view of the group would be. I know what my own view is.

This is an issue that arises.... It's the exception for policy advice to a public body. There was a particular case involving the College of Physicians and Surgeons where they had an expert opinion they gathered during an investigation where they were trying to decide whether to go ahead with the investigation of a physician. They had an expert opinion, and then I think what happened was that they decided not to go ahead. Then the complainant, after the fact, wanted the expert opinion — maybe just to evaluate their decision or maybe because she had some civil case. I'm not sure. Anyway, that eventually made its way through to the B.C. Court of Appeal, and the court said that the expert report is expert advice to a public body, and therefore it's protected under section 13 and the complainant can't get access to it.

Now, I have briefly looked at the Freedom of Information Association's submissions on this, and they make some good points, although I think they might go a little too far. They're asking the committee to consider recommending that section 13 be reworded so that it apply only where the advice is the form of an actual recommendation for a course of action. That might make sense in the traditional government milieu.

From the point of view of a professional college — and I am speaking from their point of view, because I act for professional colleges — that particular decision in the B.C. Court of Appeal, they felt, was correct and appropriate. When they get an expert opinion in the course of an investigation, it's often being used in order to try and bring about a negotiated resolution with the member or the professional involved. They will sometimes put the expert opinion to the person and say: "Look, you messed up here. You're going to have to do some education or whatever." Oftentimes that's persuasive, and the member will take the view of their colleague or peer and say: "You're right. I've made a mistake. I'm going to have to do X, Y and Z."

That resolution is the best way to deal with professional misconduct from their point of view, because if the member buys into it and accepts that they've made a mistake, all the better. That's going to be the most useful way of dealing with it. However, if the member knows that, for example, the complainant can get a copy of that expert report and use it in a civil case against them, they're a lot less likely to accept a mediated kind of resolution.

From the point of view of professional colleges, at least the ones I act for, I think they would say that the amendment that FIPA is suggesting goes too far and that maybe some amendment is appropriate, but perhaps there could be some recognition to professional

colleges that have that particular issue to deal with. It may arise for other public bodies. I don't know, because I only act for certain ones. But those are my thoughts on that.

**J. MacPhail:** Thanks. That's very helpful.

**B. Lekstrom (Chair):** I'll look to other members of the committee if they have any questions of Tamara at this time.

Tamara, you began your presentation talking about the time frames and the response times. I just want to get my head around that. Under the act, the frustration that you expressed that many of the people are feeling because of this time delay.... Are they meeting the guidelines under the act, or is it the extension request we're talking about?

[1130]

**T. Hunter:** These are two different issues, and I'll clarify that. There's a huge frustration with public bodies not meeting the basic 30-day response time for responding to an access request. I have to say I find this more with governmental departments than anyone else. They almost always take the further 30-day extension, and so it's 60 days. Even then sometimes they're not meeting it, and you're writing to them and complaining, and they're saying: "Sorry, resource problem." Even if you complain to the commissioner's office, they'll certainly have someone call them on your behalf, but there is only so much they can do about it.

That's a huge level of frustration, but that's not what I was talking about in my presentation. What I was talking about is that in the commissioner's office, once a case goes there, they used to be faster in dealing with it than they are now. I don't think it's through any fault of their own. They seem to me to be very dedicated, balanced, fair-minded people. I just think they have a huge caseload, from my discussions with them and with colleagues.

There's a 90-day period where you try to mediate a resolution to a case before it goes to the commissioner for an inquiry. If you can mediate a resolution, that's usually what everybody wants. But I'm finding that it's getting awfully close to the end of the 90 days before the portfolio officer has time to really get into the case and be able to engage at a level that will bring about a resolution. Then you're kind of up against this deadline where, unless everyone agrees to extend it further, you're going to have to do submissions to the commissioner. That represents a cost to my clients, and it would be better if we could mediate it earlier in the 90-day period.

I'm just saying that if the commissioner's office had a budget increase, they wouldn't have such a huge caseload with each portfolio officer, and those things could go more quickly. They did go more quickly in the past.

**B. Lekstrom (Chair):** Thank you very much. I will look to members of the committee if they have any further questions of Tamara.

Seeing none, Tamara, I would like to thank you again for taking time out of what I'm sure is a very busy schedule to come and present to our committee today.

**T. Hunter:** Thank you for the opportunity.

**B. Lekstrom (Chair):** All right. Thank you.

Our next presenter before the committee this morning is Dr. David Flaherty, who is the former information and privacy commissioner of British Columbia. I would like to welcome you. Good morning.

**D. Flaherty:** Thank you very much.

I don't have a prepared statement for you, probably because I'm a lazy consultant, a retired academic. I'll simply talk with you, if I may, for a few minutes and respond to any comments and questions that you have.

**B. Lekstrom (Chair):** All right.

**D. Flaherty:** I think only Ms. MacPhail was in the Legislature when I was the information and privacy commissioner, so I want to remind you of my background. As of next September, it will be 40 years that I've worked on privacy issues since I was a young graduate student at Columbia University and Alan Westin, the American privacy guru, introduced me to the subject. Twenty-five years ago I started testifying before the House of Commons in Ottawa about the importance of freedom of information. I've done that kind of testifying in the United States, Canada, Australia and New Zealand. I continue to do that kind of thing.

I had the privilege of being the staff person for the first review of the federal Access to Information Act. Murray Rankin and I, from '84 to '87, were the staff people who wrote a report published in 1987 called *Open and Shut* on the need to revise the federal legislation. Then in '93 I had the chance to become the first information and privacy commissioner for this province — a six-year, non-renewable term.

Since then I have become a retired academic. I taught at Western for a long time. I'm on the faculty at UVic, but I don't do any teaching. I'm a consultant who works basically in freedom-of-information and privacy issues in Canada and abroad — mostly on privacy. But I did advise the government of Jamaica this year, for example, on the implementation of their legislation.

I think that David Loukidelis, my successor, and his staff have been doing an excellent job of continuing the work that my colleagues and I started from '93 to '99. Certainly, on technical and specific issues — some of them of the sort that Tamara was just discussing with you — I defer very much to his experience and judgment and the decisions he wrote with respect to how these matters should be handled.

There are essentially four areas I'd like to speak to you about. One has something to do with the freedom-of-information act at the federal level. The feds, less

than 18 months ago, published a great big, fat spanking report called the *Report of the Access to Information Review Task Force*. Access to Information is what they call the federal freedom-of-information act — our Freedom of Information Act. It's a several-hundred-page report plus 29 research papers. Myself; Colin Bennett, your next witness; Murray Rankin; and others in B.C. were advisers to this committee. I certainly did consulting work for them.

[1135]

But forgetting that, this is a heck of a good piece of work. I brought it to the attention of your staff. You'll be delighted to know I'm not going to read you all of the hundreds of recommendations, but our tax money was used for this document, and it's available to your staff. You should be mining it for the kind of experience that this exceptional task force of public servants brought to their work. Essentially, the problems we have with freedom of information at the provincial level are exactly the same as at the federal level.

They made a lot of very fine recommendations, very intelligent recommendations informed by common sense, about a culture of openness, about an information management strategy for the federal government. Andrée Delagrave, who's a Justice lawyer, was the director of that task force. An idea I've given to Mary Walter, one of your staff, who seduced me into being here in the first place, is to bring Ms. Delagrave out here to talk to you about what they found. An alternative is for your staff to simply go through here and say "Here's what's relevant to our work in B.C. as we look at our ten-year-old or 11-year-old legislation and how we need to improve it." So I leave you with that idea.

The second area I'd like to address is the fact that FOIPPA is now an old piece of legislation. It's not as old as the federal Access to Information Act, which goes back to 1982, or the federal Privacy Act, which goes back to 1975, '76 or '77. Our act was built upon the Ontario Freedom of Information and Personal Privacy Act, which was drafted between 1985 and 1987. The government of the day, here in B.C., took that act in the early 1990s and improved on it. Then Alberta improved on our improvements.

FOIPPA is still an old piece of legislation now. It's 11, 12 or 13 years old. I'm particularly referring to the privacy side of it, which is what I want to address in the remainder of my remarks. Our FOIPPA has been overtaken by two pieces of legislation. Let me say, before that, that I gave you this lovely poster, because I think I'm a poster boy — ha ha.

There are ten principles on here that are relevant. All you need to know about privacy is that there are these ten privacy commandments. What I'm going to suggest to you is that all of these are in all of the legislation around the world, the 40 countries that have this kind of legislation. Whether it's for the public sector or the private sector, it's all built upon the ten privacy commandments. This particular poster comes from Industry Canada, courtesy of John Manley, who was

the father of the Personal Information and Protection of Electronic Documents Act, which is the federal act for the private sector.

I'm delighted that our Legislature followed up last fall by introducing son or daughter of PIPEDA, our own B.C. PIPA act, which takes this federal legislation and customizes it for our own purposes. What has happened is that we have this old piece of legislation in B.C. called FOIPPA on the privacy side, which I would argue has been overtaken by the Canadian Standards Association model privacy code, which dates from 1995.

When it came out, I was the commissioner. I said: "This is just wonderful. If it's so wonderful, let's give it the force of law rather than just having it being a set of general recommendations." That's essentially what has happened in PIPEDA, which is 2001 and which is now completely in effect for the private sector in Canada except in Quebec, British Columbia and Alberta, where there are specific provincial laws in place that are thought to be substantially similar to the federal act. I believe quite strongly that our provincial act, the PIPA legislation, is substantially similar.

Now, what's the problem? Where am I going with all of this? My view is that the ten privacy principles in our FOIPPA are okay in six cases and are weak in four. I would suggest to you that the accountability, the openness, the consent and the security provisions in our FOIPPA need to be beefed up and brought to the PIPA standard. I'm playing a game with you. In a sense, I'm being a privacy advocate, which I still am. I'm not just a privacy consultant. I'm saying, well, if you're willing to give our citizens and residents of this province privacy rights vis-à-vis the private sector that are as strong as they are — especially, for example, on the consent side — why don't we have it vis-à-vis the public sector, which is so broadly covered by our legislation, including schools, universities, hospitals, Crown corporations and government ministries?

I think there's a real chance for you to put some meat on the bones with respect to these four principles in PIPA and in FOIPPA that are not very well developed.

[1140]

A year ago I gave some advice to our Ministry of Health Services on the outsourcing process that is underway, and on their website they have the advice I gave them. If you're going to outsource, here are the criteria you have to meet. There's an appendix to that document which lists the ten privacy principles in FOIPPA, in PIPEDA, and then looks at the implications for outsourcing. I didn't bring that to you. I have a copy here. I wasn't smart enough to do the extra work to edit it to be really useful to you. What I suggest you do is ask your talented staff to take out the third column, "Implications for Outsourcing," and put in what PIPA actually says. You'd see under each of the ten principles: here's what FOIPPA says; here's what PIPEDA, the national privacy standard for the private sector, says; and here's how we've improved on PIPEDA in our own B.C. PIPA.

While the constitutional standard has been, "Is PIPA substantially similar to PIPEDA?" in order to have the feds acknowledge that our act takes jurisdiction in this province, I also found — in some work I did for the government in giving them advice on this issue — some substantial improvements in PIPA. We were smart enough — our drafters, the people who worked on this legislation, one of whom is in the back of the room, Sharon Plater — to improve on PIPEDA and not only make it substantially similar.

What I'm suggesting to you is that you get yourself a nice table which will show you rather quickly what's good and what's bad about these pieces of legislation and, in particular, what's weak in FOIPPA. I'll give you one example. To those of us who are fans about privacy protection and freedom of information, openness is critical. My friend and colleague, Colin Bennett, likes to say that the principle of privacy protection is: "Say what you do with personal information, and then do it." The important point is saying what you do. Under FOIPPA, with respect to openness about information practices, there's no requirement. There's simply no requirement in the legislation, whereas PIPEDA and PIPA say that an organization has to tell people what it's going to do with their personal information at the point of collecting it. That's essential and valuable.

If I turn to the consent standards — and of all the ten privacy principles, consent is by far the most important — there is essentially no consent requirement in FOIPPA. It's exceptionally weak; whereas anybody collecting personal information from us now in the private sector in British Columbia, which includes not-for-profits, has to get either our express consent or implied consent to use our personal information, which is exactly what it should be. But the government, basically, is not faced with that kind of an obligation, so I feel that's an area you should address in your work. I'd be quite happy to help your staff if they need any assistance in formulating the table that I think would be quite helpful to you.

The third area I would like to address has to do with my evolving thinking about how to manage privacy properly, which I do for a lot of companies, especially in the health field, and for a lot of national agencies and so forth. Last summer the Ontario Hospital Association had an e-health privacy and security working group, which published a report on guidelines for managing privacy, data protection and security for Ontario hospitals. I was basically the principal author of that report. In the course of that work, I developed what for me was a new formulation of privacy management. I call it privacy management plans, and it's laid out in that report. What are the components of a privacy management plan? This would apply to any company that is privacy-intensive or to a hospital or to whatever you can think of — the Ministry of Health Services, for example, or the ministries of Finance and of Provincial Revenue, etc.

Here are the kinds of things I think should be in a sound privacy management plan. Basically, they're not

present in our FOIPPA legislation on the privacy side, but they are in PIPA. PIPA basically requires many of these things for the private sector. First is to have a privacy officer in place. Somebody's got to be responsible for the shop. You'll find them in place in many government ministries, but they are primarily preoccupied with the freedom-of-information side of their work and not the privacy side. I think it's essential for privacy teams to be created in these big organizations on a part-time basis essentially to help the organization — in the provincial government, in the Crowns or whatever — manage the privacy issue properly. The various parts of an organization — including public relations, IT, legal, communications, straight management and database operations — come together on a periodic basis and keep their eyes open for privacy issues in the meantime so that they can actually address these issues and solve these problems before they become public relations problems for the government ministry.

[1145]

The idea, first, is having a privacy officer in place, a privacy team, having resources available for training on the privacy and freedom-of-information side — I'll come back to that later; that's my fourth area I want to address — and promoting the adoption of what we call PETs, or privacy-enhancing technologies. If we're going to use as many technologies as the government is now using to collect, use, disclose and retain personal information about us, we should be using as many privacy-enhancing technologies as possible. We should always be considering that. I think you should amend the legislation to simply say that in every instance where public bodies are going to collect our personal information and use and disclose it, they should be considering things like encryption or anonymization of personal information before it's disclosed or when it's stored. There's a whole set of these privacy-enhancing technologies that are available, because just as the Web and Internet and everything else are developing, so are techniques that could be used to protect the personal information of individuals.

I also think we need to address in FOIPPA more carefully than we have in the past the whole issue of information consent. I'm making a very conscious formulation by talking about information consent rather than consent for treatment, especially in the health care field, which is my specialization nowadays. We've always paid attention to consent for treatment, but we haven't paid enough attention to information consent.

I'll use the example of a doctor's office. May I remind you that doctors' offices in B.C. are now covered by B.C. PIPA, which is quite something given the strength of the requirements. I was in a doctor's office yesterday, and I simply dictated to the physician, who was an ophthalmologist, a statement that this office collects, uses, discloses and retains personal information in compliance with the B.C. Personal Information Protection Act — period. He said he'd have the sign up in his office tomorrow, and I thought: "That's good." I offered, because I wanted a quick appointment for a

certain service, that I'd give him free privacy advice for a few hours, and he and I got along just fine.

Rogers' Chocolates or the Canadian Blood Services or the Canadian Institute for Health Information working in British Columbia, or a charity, now has to tell you: "We're collecting your personal information. We're going to use it, disclose it and retain it in compliance with this B.C. act. If you want to know what it means, the government has a website that'll tell you one of the things you should do." That website includes guidance on how to have a privacy officer, how to put up a notice of some sort, how to get express or implied consent.

The express consent is quite interesting. I just want to tell you what my view of the world is here. The first time you sign up with a doctor.... Most of us would be quite happy to get a family doctor in this country nowadays, so we'd practically listen to anything they told us. They should be telling you, the same way a bank does: "Here is our privacy policy. You should understand what our privacy policy is, and you should ask questions about it. If you have any questions, go to our website or ask our nurse or clerk, or ask the doctor and he'll explain it to you." Every time I come back to that doctor's office — and I've gone to the same physician, thank God, in Victoria for ten years — I am giving implied consent for the use of my personal information.

The first time you sign up for the service, you should be giving express consent for the service. Then keep coming back and it's always implied consent, especially for that period of health care.

Another component of a privacy management plan that I want to emphasize to you is intelligent and meaningful confidentiality agreements. Now, I must have looked at the confidentiality agreements used for public servants when I was in government, but I don't remember them. Mostly, they're verbiage, they're legal gobbledegook, and people have no idea what they're signing. They sign it the day they get their parking pass if they get a parking place, their social insurance number, their agreement to get paid and so forth. What I argue with my clients in the public and private sectors is that you have to have meaningful confidentiality agreements that the people signing them can understand. What that means is having available to your staff and your employees frequently asked questions about what confidentiality agreements mean.

My model client in a lot of these things is the Canadian Institute for Health Information. It's the national health statistics institute that basically takes care of health information data from hospitals and lots of other places and produces hospital reports and health utilization information. If you were to go to their website, you would see that they have on the website not only a privacy policy but frequently asked questions about what CIHI does with personal information and also privacy impact assessments for almost all of the 16 major databases that CIHI holds. Someone wondering, "Just what does CIHI do with my personal information?" can go this website, as they should be able to go

to the website of any government agency in B.C., and get some guidance as to what the Ministry of Health Services or the Vancouver Island health authority does with their personal information. What are its privacy policies? Where do I go if I want to make a complaint? How will it be handled? Okay, enough on the whole idea of privacy management plans.

[1150]

I want to preface my last area of remark by saying that I'm a taxpayer. I'm delighted that the government is trying to balance the budget. I'm not happy with the deficits we have in B.C. or federally or the debt we've amassed. I'm of an age where I worry about my children, and all that kind of thing.

At the same time I'm very concerned — and it will not surprise you — at the funding or the lack thereof for all the activities dealing with the implementation of the Freedom of Information and Protection of Privacy Act. When I was an officer of the Legislature, we used to say that all our budgets together were one-tenth of 1 percent of the budget of the province of British Columbia. It's a pittance in the overall whole.

I not only think it's very important to fund the office of the information and privacy commissioner a lot better than it's currently funded, but I also think it's important that central government fund its ministries and those responsible for implementation of FOI and privacy a lot better. I'm not going to name names, but the cutbacks are so serious that there's nobody minding the shop with respect to privacy and freedom of information in most ministries of government. Now, that's an excessive statement, because there's probably a boss with the title glued across their forehead, but he ain't got no resources. They've got no capacity to train.

It's a walking time bomb for the government in terms of privacy crises and privacy disasters that then cost a lot of money to manage. You're familiar with the problem of political disasters. We're also able to have privacy disasters and privacy crises. It's not that expensive to manage, but just as there has to be a fundamental commitment to open, democratic government and a reminder that access to information is a fundamental democratic right in our society....

The most important change in our democratic system — I'm a historian by training — in the last 20 or 30 years in Canada is clearly the Charter of Rights and Freedoms. But I would argue that in the last 25 years, the other most important democratic change we've had is the introduction of access to information legislation — what the provinces call freedom-of-information legislation.

Nobody loves it. I didn't like being the commissioner and reading about my expense accounts on the front page of the Vancouver *Province* — especially when a lot of what they reported was what I thought was bullshit — but I accepted the fact that my expense accounts and everything else should be publicly open and accessible. As a consultant for the federal government or the provincial government, I accept that the contracts I have are open, any expense accounts I submit are open, etc.



The irony of all this is that now the other commissioners are being so careful. I mean, there was a time when you could have a good meal with the privacy commissioner of Canada. Now, you'll be lucky to get to Subway with him, and it'll then be on their website immediately. I take them to the meals rather than going to Subway with them. That's the way it should be, because you're spending public money.

I also think that if you look at the government's ministry of... I forget what it's called, but it's got the corporate privacy and information access branch. It's the ministry of government services.

**J. MacPhail:** Management Services.

**D. Flaherty:** Management Services. Thank you, Ms. MacPhail.

I just did some work for them. They paid me. It was all very nice. They don't have any money. Here they're supposed to be the central government office seeing that privacy and access to information are properly managed to keep the government out of trouble, and they don't have the resources. They can't do the training they should be doing.

I'm not trying to claim I'm a big expert on their budgets or anything like that, but I know from anecdotal information that these people need to be resourced to do the work that they're trying to do.

I'll end by simply saying to you that I mentioned access to information as a fundamental democratic right. When you're talking about this privacy and data protection stuff, this is not just any old thing going on in government, as important as all the other things going on in government are. This is a fundamental human right. We have a fundamental right to privacy in Canada based on the Charter of Rights and Freedoms. Our Legislature, in its wisdom, has chosen to take this concept of privacy and apply it to the data protection area by this FOIPPA legislation, which I think needs to be strengthened particularly in the important work that this review committee is doing.

At the end of the day, you have to remember that we are dealing with democratic rights with respect to freedom of information and fundamental human rights with respect to the invasion of privacy and protecting against the invasion of privacy.

That's what I have to say, and I appreciate the opportunity to speak with you.

**B. Lekstrom (Chair):** Well, thank you very much, Dr. Flaherty. For us, it's definitely a huge asset to hear from somebody who has been so involved with this issue not just in British Columbia but right around the world. I thank you for taking the time.

I'll begin with questions from members of the committee.

**J. Bray:** Thank you, Dr. Flaherty, for your presentation. I sit on several committees, and lots of people

come with written presentations, but they're rarely as succinct as yours was. I appreciate that.

[1155]

There's an area that I'd like to ask your counsel on. You talked a bit about consent. You're talking about PIPA versus FOIPPA. This is my take on it. If I go buy a pair of jeans from Bootlegger and I'm giving my address to the clerk so they can mail me promotional stuff, it's likely that what they might do with my information is sell it to other mailing lists. The perceived use of that information is still relatively limited to the marketing and merchandising type of thing.

It's easy to say: "Here's explicitly what we are going to do or not do with your information. So will you consent to it?" With government the issue becomes that you as an individual British Columbian may have several entry points into government. As new benefits or new opportunities come on stream that weren't conceived of the day you filled out your MSP application or your income assistance application or your whatever it was....

First of all, my question is: can you write a consent that would be logical and defensible to say, "If it's in your interest to now get an initial benefit and if we can share your information with the Canada Pension Plan or HRDC for your child tax benefit, do you consent in a way that says we didn't conceive of it two years ago when you applied"?

The second question is.... I was involved with the Ministry of Human Resources when we had to change our consent plan because we were doing more data sharing. The consent form was longer than the application form. As you say, the issue became that it was all legal gobbledegook that was based on lawyers saying, "This is how you cover yourself," but no worker understood what the form was at the end of the day and could not provide clarification. Do you have ideas on how you can provide legally defensible consent but actual consent that works in the real world?

**D. Flaherty:** Some of you would be familiar with the fact that first nations in Canada have been asked — there are about 730,000 of them — to fill out a consent form for non-insured health benefits, which is the \$6 billion a year Health Canada health insurance service for aboriginals. I wasn't primarily giving them advice on this, but I said, "Yes, getting consent was a good idea because for 20 years you've been collecting personal information under the federal Privacy Act, which says you should get consent," and they hadn't been getting consent. They ended up with a three- or four-page consent form, the lawyer's one, plus a consent booklet that was completely impenetrable to the first nations population. I'm a privacy pragmatist, not a privacy fundamentalist. That's exactly what you don't want in our society.

The model consent form, the information consent form that I prepared for Ontario hospitals, which is being used by the University Health Network in Toronto — the teaching hospitals at the University of To-

ronto where my client is, Cancer Care Ontario — is one page. It tells people from a health care point of view: "We use your personal information for direct patient care; administration and management of the health care system; research, teaching and statistics; and complying with legal and regulatory requirements." I thought that was fully informative for the individual. Here's one page: "If you need a paragraph or a booklet or a website or an 800 number, we can provide you with that if you really want to search out exactly what will happen."

If you go to the Air Miles privacy policy on line or RBC or Air Canada Aeroplan, you will see that they state: "Here are the reasons we use your personal information. Do you agree with this?" Basically, the reality is that you don't have any choice. If you want to have a bank account, you've got to agree. If you want health care, you've got to agree. The job of the privacy commissioner is to make sure that these information consent documents are meaningful, intelligible, accurate and also reflect the possibility of some enhancements. Clearly, we don't want a situation where some person is getting some type of benefit in our society.... If the Legislature comes up with a new benefit, we shouldn't have to sign everybody up again. That could be handled by a notice requirement.

One of the nice things in our B.C. PIPA legislation and in the new Ontario Personal Health Information Protection Act that they introduced a month ago and started hearings on two days ago, Bill 31.... It allows notice to fulfil many of the obligations of getting consent. The Canadian Medical Association has published a very nice poster that tells patients coming into a doctor's office: "Here's what we're going to do with your personal information. Here are the main uses. We're going to get you to consent when you sign up to the practice the first time, etc."

[1200]

I don't want to claim I've sort of thought through exactly how a big ministry would do this. Fortunately, in the health care area most of the work is done in hospitals or doctors' offices or labs or pharmacies, so the burden of consent is on them. Private pharmacies and labs like MDS are covered by PIPEDA, so they've got to get your consent, expressed and implied. I don't want to filibuster you on this issue, but those are my thoughts at the moment.

**J. MacPhail:** Thank you very much, Mr. Flaherty. I certainly appreciate your advocacy around privacy, and I think that is something that our committee is going to look at.

I actually want to seek your expertise but also your advice on the freedom-of-information side of our provincial legislation, and I'm going to explore it on two fronts. One is around consequences arising from the budget — but I'm not emphasizing that — but also two of your privacy commandments that I would suggest.... I know they're privacy commandments, but I would say that they're commitments made around

freedom of information too. They are openness and then challenging compliance.

At our hearings last week one of the presenters told us about a report that an Alasdair Roberts had presented around FOI requests here in British Columbia, and it was the first that I think any of us had heard about this report. It had been released over Christmas. I went and looked at it, and then I followed up with some reports that Ann Rees, a local reporter, had done via a scholarship around, I think, federal FOI and also Ontario FOI.

If I could, Mr. Chair, there are two areas I want to explore. One is that the British Columbia government has set up a tracking system of freedom-of-information requests that this researcher, Alasdair Roberts, said is leading to consequences that.... Money is being spent by this government out of Management Services to set up what they call a corporate request tracking system, and it's part of a department that I've never heard of before — corporate privacy and information access branch. That branch, which is substantially funded but not reported — and I've never had an opportunity to discuss it in the Legislature — tracks requests made and then gives them a sensitivity ranking.

Some of the results of the sensitivity rankings that this fellow reported on were that virtually.... Let me just see here now. Media requests are tagged as highly sensitive almost 90 percent of the time. Political party requests are tagged as highly sensitive almost 90 percent of the time, and then it goes down from there in terms of.... Oh, sorry. Political parties are tagged highly sensitive 89 percent of the time and media 72 percent of the time. So that's one. I want to talk to you about equality under the law.

The other aspect that Ann Rees demonstrated in her examination of this issue is that there is all sorts of research that she's gathered that points out that this tracking system really leads to people being treated differently under the law and that it was never the intent of the freedom-of-information legislation. I'm looking into this because, having been a person who was often, I guess, properly blindsided by freedom-of-information requests — some of which came from my colleagues sitting around the table with me right now, and I say rightly so, frankly — I'm now concerned that my opportunities as a new opposition member are being limited by this tracking.

The other consequence that flowed from Alasdair Roberts's study of this new tracking mechanism is that requests labelled highly sensitive take more than double the time to fulfil. I'm just wondering whether you could comment on whether this is pervasive. This tracking mechanism by this government — what is your advice in terms of the original spirit and intent of the law?

[1205]

**D. Flaherty:** I am not that familiar with how things that are going on work today, Ms. MacPhail, but my recollection is that your own government had a track-

ing system pretty much the same as this government must have for what we would have called sensitive requests. I have no objection, as a former commissioner or as an information and policy consultant, to the government understanding that the same request is being made to 40 different parts of government. It might as well be handled properly or managed effectively, and it's the job of this corporate privacy and information access office to do it.

I think I have the highest regard for Alasdair Roberts, who is a Canadian who teaches. He was at Queens and is now at the Maxwell school at Syracuse University. He's the guy who really gets down and dirty with this FOI stuff, and he actually knows what's happening in the trenches. I would give great credibility to his findings.

Ann Rees I have less enthusiasm for. I'm saying this with a smile, simply because she was the author of my expense account stuff on the front page of the *Vancouver Province*, so you will forgive me for being.... I've always claimed in public she's my favourite B.C. reporter for this reason. She has spent this year on a fellowship — a Southam fellowship, I think — and she, again, knows what's happening in practice.

One of the important findings of this federal access task force is that we depend heavily on the media to exercise our access rights. That's the way it should be. There's nothing inappropriate about that. So media requesters.... I don't see Russ Francis here today, but I regard him as a patron saint of FOI in this province. He keeps his eye on that stuff. He understands it. I had to manage him when I was commissioner, I will admit, but he's one of the people who really make this system work.

At the federal level, people like Andrew McIntosh of the *National Post* and Jeff Sallot of the *Globe and Mail* and the researcher whose name escapes me at the moment, who gets a lot of the stuff for them.... That's exactly what should be done. My solution to all of this, were I ever, God forbid, a cabinet minister.... I would tell my ministry, my staff: "Put everything we do, as soon as it's finished, on the website."

My model in this regard is the Canadian Blood Services. Because they've had such tragedies in the past, if there's an inspection of one of their labs by Health Canada, within a month that inspection and Canadian Blood Services response to it are on the website. The solution in government is to be proactive in terms of getting the stuff out there. The reality is that if you get the stuff out there, there's no story. If it's available to every media person, there's no story whatsoever. The letter you receive that morning and the response to it may not get on the website that day, but the solution is to get the stuff out there and be proactive in creating a culture of openness with respect to open government. I think that's all I can really say, Ms. MacPhail.

**J. MacPhail:** Okay. I just want to bring to your attention.... I appreciate, Mr. Flaherty, that you're moving on to the privacy side, but then I noticed, I think, an official from the Ministry of Management Services

nodding that the previous government had such a system. Actually, no, the previous government didn't have a system of ranking highly sensitive, medium sensitive or not sensitive at all. We did track requests. We tracked requests for timing of fulfilling of those requests, and we tracked cross-government requests to make sure that all government agencies were approaching a single cross-government request in the same fashion.

This government has actually hired EDS, a corporation, to set up a very formal tracking system, and they attach each request with a rating. This is brand-new. It was simply not done by the former government. I have concerns about who's actually doing the tracking, because one of the things that this Alasdair Roberts report says is.... I'll just read it, Mr. Chair, because I am going to be pursuing this as an amendment to legislation. "In general, the CPIAB" — which is the corporate privacy and information access branch, which is set up by the Ministry of Management Services — "sensitive tag did not increase processing time if a ministry had already classified the request as sensitive. On the other hand, it did increase processing time if a ministry had not already classified that request as sensitive."

[1210]

You now have this government set up a very formal computerized tracking base — brand-new. They've invested a substantial amount of money in this, and this central agency is changing the sensitivity ratings of fulfilling requests that a ministry might have made. I can't find out who's changing those ratings. I don't know whether Martyn Brown of the Premier's office is involved in them at all. I can't find out. There's no mention of this agency in the government's performance measures. There's no mention of this in their service plan. There was no mention of it in their budget whatsoever. In fact, Mr. Roberts says that this particular agency goes far beyond any of the federal tracking systems that you have just referred to as well.

That's why I bring it up. I hope at some time — and your expertise is, I know, in great demand.... Even though Ann Rees.... She also revealed stuff about me on the front pages of the *Province*, so I understand that. Yeah. It is under an Atkinson Fellowship in Public Policy investigation that she did this study, which has come to some pretty troubling conclusions. If you do have a mind to turn to either of these studies, I'd sure appreciate it, because I am going to pursue this matter in terms of an amendment in the Legislature about equality under the law.

Mr. Chair, just as a point, I might say that both Alasdair Roberts's and Ann Rees's reports are so interesting in terms of this new agency of freedom of information and how it relates and who gets their requests filled how. I would actually hope that we can invite them as witnesses to our hearings, because certainly their information and their studies are completely fresh, and they would have some very interesting information to present on the freedom-of-information side of legislation and the changes demanded.

**B. Lekstrom (Chair):** I'm going to look to other members of the committee to see if they have any further questions.

Seeing none, Dr. Flaherty, I would like to thank you again for taking the time. I think you've raised a great amount of interest and helped our committee gain some understanding of what I feel is a very important piece of legislation for the people of British Columbia. I thank you very much.

**D. Flaherty:** Thank you.

**B. Lekstrom (Chair):** We will move to our next presenter today. With us we have Dr. Colin Bennett, who is a professor with the University of Victoria. Welcome, Dr. Bennett.

**C. Bennett:** Thank you very much, and thanks for the opportunity to talk with you today. I'm a current academic, unlike Flaherty, so I have to be a little more scholarly than him — all right?

I want to talk to you entirely about the privacy side of this legislation. I have spent a good deal of my career studying privacy protection and studying the ways in which different governments and different societies have tried to address this incredibly important problem. As a result of that analysis, I've drawn some conclusions about what works and what doesn't work. I hope some of that information might be useful to you in your deliberations.

I'm also one of the few individuals in this country who has made a formal complaint under the federal Personal Information Protection and Electronic Documents Act, PIPEDA. I draw some conclusions about that as well. I think my remarks have been copied for you, so you can follow what I have to say.

The importance of privacy protection has been growing steadily over the last 30 years or so, as many innovative and intrusive technologies have entered our public and private institutions. A lot of new practices — video surveillance cameras, biometrics, smart identity cards, drug testing, telemarketing, genetic data banks, etc. — have unintended consequences for the protection of personal information. These developments have raised the fears of citizens in every state, including British Columbia, that their privacy is being attacked from a variety of institutional and technological forces.

[M. Hunter in the chair.]

A much-publicized former privacy commissioner of Canada, George Radwanski, was fond of saying that this is the defining issue of the next decade. I wouldn't go that far, but it's nevertheless an issue that's always in the newspapers and at the attention of government.

[1215]

Surveillance practices are changing in kind as well as degree. Thirty years ago we were normally aware when we provided personal information. We filled in a

form. Now the process of information collection is a lot more surreptitious. We leave traces of personal data behind us when we go about our everyday lives — booking a hotel or an airline, browsing the Internet, sending an e-mail, crossing an international border, going to the doctor, etc. In our roles as citizens — employees, travellers, patients, students, recipients of social benefits, whatever — we continuously and unawares leave fragments of our data behind us when we go about our normal lives.

[B. Lekstrom in the chair.]

These developments have forced experts to rethink the way that privacy laws are drafted and implemented. FOIPPA was a state-of-the-art piece of legislation in 1992, and in some respects it's now outmoded, as it was based on an understanding of information technology as it was in the 1980s. I want to just suggest some ways that we might rethink the privacy provisions in the light of these new technological developments.

The committee's review is also very timely, coinciding as it does with the application of the new Personal Information Protection Act, PIPA, which came into effect in January. I'd like to congratulate the government for this initiative. I think it's very, very important that B.C. was one of the first provinces in Canada to pass substantially similar legislation under the new federal legislation.

Despite the importance of privacy and despite the fact that it's always in the news, when people think of this legislation that you're reviewing here, they think more about FOI. When one looks at the stats of the number of requests to the B.C. commissioner for reviews of FOI requests versus the number of privacy complaints, the imbalance is quite remarkable. According to the table that I looked at on the commissioner's website, there's really a small handful of orders that have touched on the privacy protection provisions, and these on further research are really quite ancillary issues. There is some data there from his last report. He reported receiving just under 300 privacy complaints versus over 800 requests for review of FOI requests in 2002-03.

This committee has received and will receive a great deal of advice about the wording of FOIPPA, and I want to suggest a few amendments to you about the definitions and about various exemptions. One of the principal messages I have for you is that the success of a privacy protection policy in government and the private sector is only partially dependent on what the law says. I think this is one of the conclusions that a lot of us have reached over the last 20 years or so. There are a lot of other, more critical factors that need to be taken into account when you try and determine whether the privacy of citizens in a particular jurisdiction is in fact protected. I note just four different factors that I think we should keep in mind.

The ability of the privacy protection regime to encourage the voluntary adoption of information privacy

principles. In other words, the goal requires organizations to see that this is an important value and to build privacy protection from the bottom up rather than just the top down.

Secondly, the use of the entire repertoire of possible policy instruments. These hearings are concentrating on the content of the law, but it should never be forgotten that any privacy protection policy has to rely on other things — codes of practice, privacy impact assessments, privacy enhancing technologies that David Flaherty mentioned to you. Each of those is a necessary condition for the success of a privacy protection policy.

Thirdly, on the ability of the privacy commissioner to apply an ounce of prevention. As drafted, FOIPPA gives the impression that the most important responsibilities of the commissioner under this legislation relate to complaints investigation and redress. In my view, this is one of the least important functions of privacy commissioners. The complaints investigation process is largely a reactive one, performed only after privacy problems arise. So the implementation of privacy protection law is as much an educational effort as it is an investigative one. Much can be achieved, therefore, in anticipation of policy and legislative developments and system development if privacy protection is built in at the outset rather than added on afterwards as a result of complaints and investigation. Therefore, the most crucial powers that I think you can give a privacy commissioner are those that are general and those that are anticipatory rather than those that are specific and remedial. So I've got some suggestions about how you might want to look at revising the law in that respect.

[1220]

Finally, it's questions of policy harmonization. This legislation does not stand in isolation. It's intimately connected with other provincial legislation, with B.C.'s PIPA, with the federal laws, etc. Therefore, a more important issue today than it was perhaps ten or 20 years ago is the extent to which the provisions in this law are consistent with what is said in other laws, given the ease with which personal information can be transmitted across jurisdictional boundaries, both provincial and international.

Just a few recommendations for you. David Flaherty mentioned the importance of consent and notification, and I'd be happy to answer questions about that, but one of the most important principles of a privacy law is transparency. It's being open. It's for an organization to say what it does and do what it says. Saying what an organization does and why it needs personal information is critically important. The citizens should know why information is being collected, how it will be used and so on.

In my view, FOIPPA is deficient in that regard, not because there are not a lot of provisions in FOIPPA about transparency, but because they're just not taken seriously. I draw your attention to section 69(2), which requires ministers to "publish a personal information directory," which includes the personal information, information-sharing agreements, any privacy impact

assessments conducted and other information considered appropriate. I don't know anybody who believes that this provision is clearly understood and implemented. I suspect the commissioner and his staff rarely, if ever, use these directories. I assume that most of them are completely out of date.

One of the problems with this section is its reliance on the concept of the personal information bank, and this goes back to what I was saying about the law being a bit outdated. That's an outmoded idea derived from a prior technological era when it was possible to define discrete data banks in which personal information was held. In today's more interactive and network computing environment, it is impossible to determine where one data bank ends and another one begins. I appreciate the intent behind this section, but I suspect that it's one of those legislative requirements that public bodies will always find a low priority, given their resource constraints.

If that's the case, I think the committee needs to look very seriously at whether those provisions should not be seriously amended and made more realistic so that public bodies can in fact publish some meaningful information on a timely basis about what personal information they collect. In this regard, it might be useful for you to have a look at the private sector law, PIPA, section 6, and consider the parallel provisions there that require bodies to develop explicit privacy protection policies.

David Flaherty mentioned privacy management plans, but what I have in mind here is more the general codes of practice that translate the privacy requirements of FOIPPA into language that both clients and employees can understand and apply them to the day-to-day operations of the public body. I think that exercise would assist public bodies in an understanding of exactly what personal information they hold and why they hold it. I suspect that it might be more realistic and withstand a better chance of being more seriously implemented than the current section 69.

Another set of ideas I have has to do with this principle about an ounce of prevention and using the entire repertoire of instruments that a commissioner might have at his disposal. Commissioners can act, as I've said, as unpaid consultants to organizations that wish to introduce new products and services that may have implications for the protection of personal information. Privacy impact statements can be an effective tool for an analysis of these implications. They can anticipate future privacy problems and encourage the consideration of privacy and security issues at the outset. It seems to me it would make sense to formalize this responsibility, granting the privacy commissioner the power to advise on the privacy implications of new information systems in both public and private sectors in this way.

Three practical suggestions about section 42 of the legislation, which I think would make the powers of the commissioner just more up to date. First, section F allows the commissioner to comment on the privacy

implications of "proposed legislative schemes or programs of public bodies." I think that should be amended to include the word "existing." It is very difficult to distinguish between existing and proposed schemes, and the commissioner, it seems to me, should have the right to provide his views in the absence of any formal complaint on any government scheme, technology or practice — existing or otherwise, proposed or otherwise — that has implications for the protection of personal privacy.

[1225]

I think that to some extent, he practically does that anyway, but sometimes I think he gets in trouble, and it would be nice if it was specifically provided in the legislation.

Secondly, Section 42 says nothing about privacy impact assessments, though they are mentioned later in the act, in section 69. PIAs are now a standard feature of most privacy protection regimes. They are analogous to environmental impact assessments, and they could be a helpful tool for public bodies to analyze the privacy implications of new technologies, products, practices, databases, delivery systems, etc., and to avoid privacy disasters, to avoid the highly publicized media attention that takes place when hard drives find their way into garbage tips and personal information gets revealed in that way and becomes incredibly embarrassing for the organizations concerned.

I have the suggestion that section 42 give the commissioner the power to require the public body to prepare and submit a PIA whenever new services are being developed that have privacy implications. Privacy impact assessments need not necessarily be huge reports. They can be very brief analyses, brief checklists which just suggest to the commissioner that the public body has at least thought of the privacy implications when it's delivering a new service.

Finally, as David Flaherty mentioned, one of the innovations in privacy compliance that has arisen since FOIPPA has been the use of privacy-enhancing technologies, or PETs to use the acronym. Traditionally, it's always been thought that computer technology is a threat to privacy. That is an outmoded notion. There is a variety of privacy-enhancing technologies — encryption systems, filtering systems, public key infrastructures, a whole list of them — which can help organizations build privacy into their organizations and the architecture of information systems. But there's no mention of technological solutions anywhere in this legislation, and they're extremely important instruments in the armoury of the contemporary person who is interested in privacy and data protection. I'm suggesting, in section 42, the addition of the power to recommend the use of privacy-enhancing technologies where appropriate.

I want to conclude, if I have a little time here, with three more general issues, which I don't have any solutions for but which I hope you might address in your deliberations. Firstly, overrides of FOIPPA. Regulating the personal information practices of public bodies —

government — is at odds with the immense power of the state in relation to the individual. In fact, governments in B.C. and elsewhere can do whatever they want so long as they duly legislate it.

There are provisions in other pieces of legislation in B.C. that override FOIPPA, both the FOI provisions and the privacy provisions. I haven't done any extensive research on this, but we did a simple search of the legislative database for bills introduced over the last ten years which include the words "despite the Freedom of Information and Protection of Privacy Act," which leads, therefore, to provisions which say that the provisions of the legislation override those provisions. There's a long list. It's a rough test, but it suggests there are a large number of provisions buried into the legislation that might override FOIPPA. I think it would be a good idea for these to be examined as part of the committee's review of this legislation. It may be that somewhere in government there has been an analysis of that, which I don't know about, but I think it's very important to recognize that those kinds of provisions can really undermine the intentions of the Freedom of Information and Protection of Privacy Act.

Secondly — this touches on Joy MacPhail's last question to David Flaherty — I have not filed a complaint under FOIPPA, but I have under federal PIPEDA. I therefore know something about the pressures that complainants are under when they take the step to challenge the practices of a large organization. I'm a little bit different from the average complainant because I have a certain expertise in this area. I speak in the media, and I have ways in which I can publicize my views.

I can quite imagine that ordinary complainants might feel under significant pressures once they put their name to a complaint or to an FOI request. Invariably, the first response of management of a public body, upon learning of the receipt of an FOI request or a privacy complaint, is to ask who has made that request. While that might be a natural curious response, it's not warranted under the act. The FOIPPA provides information access rights to individuals. They should not have to suffer negative consequences of exercising those rights in the form of a derogation of their privacy.

[1230]

The individual's identity and the reasons that individual is seeking to protect his or her privacy or to make an FOI request really should have no influence over their rights to the information. During the handling of requests, many public employees I know learn of the identity of the requester despite it not being at all pertinent to the performance of their jobs. The very system that tracks these requests, which Joy MacPhail mentioned earlier, for the supposed purpose of managing time lines often includes the identity of the requester and is available to many people who really have no business knowing that identity.

That, of course, produces a general hostility to requesters sometimes labelled as troublemakers or fre-

quent flyers. It's something I've often found troubling, and I hope you might take a look at it even though I have no sort of specific recommendations for you.

I have some final remarks about the funding of the commissioner's office. David Flaherty has already addressed those, and I won't repeat what he has to say. We're all conscious of resource constraints, especially those of us who work in universities, but nevertheless I do want to say something very, very positive about the hard-working, creative and dedicated people that have worked in the office of the information and privacy commissioner. They have gained a vast experience in this legislation. There has been very little turnover in that office, which suggests that they're very dedicated to these issues and very efficient. They deserve the resources that are necessary to fulfil these important functions — both existing functions and the new ones they have under the PIPA legislation.

Thanks very much for your attention.

**B. Lekstrom (Chair):** Thank you very much, Dr. Bennett. I am going to look to members of the committee if they have any questions. I'll begin with Joy.

**J. MacPhail:** Thank you, sir. Why is the protection of privacy becoming increasingly important for experts such as yourself and Dr. Flaherty? The reason I ask this question.... It actually is a straight-up question. When there were paper records, the improper release of personal information occurred in often disastrous ways.

**C. Bennett:** Yes.

**J. MacPhail:** Is it because we're collecting more personal information, or is it because personal information could now be put on one simple computer CD?

**C. Bennett:** I think it's both. I draw your attention to the remarks I said earlier about the ways in which personal information is being collected. I think this is important.

The issues 30 years ago, in the 1970s, typically had to do with the provision of information on forms. Take the census, for example. Whenever a census is conducted, there's a debate about the questions and about whether the questions are intrusive, etc., and those are important debates. The census is an interesting and not very typical way that information is collected about individuals. It's one moment. You see a list of questions. You know exactly what information is being asked of you. You may find it disturbing that that information is being asked of you, but there's one discrete moment when you're providing that information.

Now it's very, very different. Now information is collected about you surreptitiously. When we browse a website, for example, cookies are registered on our Internet browsers. When we use our credit cards, a trail is left.

I think one answer to your question is that individuals fear that information about them is being col-

lected without their knowledge and consent. Then all of a sudden they discover that, wow, there's an organization that knows something about them and they never remember giving information to that organization — when they receive a telemarketing call, for example. I mean, that's the most typical example. The extent of third-party collection and disclosure of personal information suggests that individuals, even though they may not have a very sophisticated understanding of this very complex value that we're talking about here, have a gut reaction when information is requested of them from organizations they thought they had no contact with and no relationship with before.

We have a string of public opinion polls in Canada and elsewhere that support those findings. There was very interesting one done in B.C. a couple of years ago.

[1235]

**J. MacPhail:** Thank you.

**J. Bray:** Thank you very much for your presentation. I'm going to go to your ounce of prevention. We had some discussion before about a suggestion of expanding the commissioner's role and whether or not that suggestion actually moved the commissioner in from an advisory role to part of the decision-making role which, perhaps arguably, is parliament's role. What you're suggesting, first of all, is that he or she may comment on existing programs as opposed to having any ability to actually out and out ban or change something simply because he or she is....

**C. Bennett:** Yes. Yes.

**J. Bray:** Okay. My second question. As a former bureaucrat, every time I see a sort of mandatory provision — the checklist form, as you say, of a PIA.... First of all, having filled out regulatory assessment sheets and environmental scans and multicultural scans and disability lenses.... Very quickly those go from being progenitors of thought to: "How can I quickly fill out the form to get this thing on to a deputy?" I ask this very seriously, because you talked about all this new technology and the risks that are inherent in it, and yet the examples you cited were of theft or somebody accidentally throwing something in a dumpster that now somebody else picked up and had a look at. Have you got examples where a lack of doing this led to serious privacy breaches because of the actual technology as opposed to an individual error or a criminal act?

I guess the issue is that I don't think the PIA will exempt someone from stealing my laptop from my ministry office if they really want to or somebody having a complete brain-dead moment and throwing something into the dumpster. A PIA won't stop that.

**C. Bennett:** It won't stop it. It will alert the organization to their processes by which they dispose of hard drives. That's the point. In terms of other examples, I

take your point. The most visible privacy disasters are like that. There was one, when David Flaherty was commissioner, about health records appearing on the beach somewhere in northern B.C.

**J. MacPhail:** I was Minister of Health.

**C. Bennett:** That's right, yes.

There are other examples, like when intrusive forms are produced without adequate consideration of how individuals are going to react to those forms when they're asked personal information. PIAs shouldn't just be checklists. They should be built into organizational practices so that whenever personal information is being collected, somewhere in the organization there's somebody who's said: "Well, wait a minute. Are there some privacy implications here?" To a certain extent that means going down the checklist — David Flaherty's ten principles — and saying: "Okay. Are we compliant?"

In addition to that, I think there are also some subjective considerations that need to be brought into it. Are people really going to get angry if we ask them for this personal information? What risks are there in terms of endangering our relationships with our clients, with our employees or whatever?

**B. Lekstrom (Chair):** I do have two speakers left. I'll go to Harold Long and then Mike Hunter.

**H. Long:** Well, Colin, on both occasions — yourself and David Flaherty — on this issue of funding the commissioner appropriately for the information and timing, how would you feel if there were extended fees or fees on these services as a way of helping the commission fund...?

**C. Bennett:** Fees for FOI requests?

**H. Long:** I mean proper fees for FOI.

**C. Bennett:** Well, there already are.

**H. Long:** I'm talking about if it's not funded appropriately, it's not a user-pay. I mean, I can take issues where we have other areas where we use services of the government and we pay fully — B.C. Ferries almost being one of them, other than....

[1240]

**C. Bennett:** Well, I guess I would respond to that by saying that I don't regard this as a service, particularly on the privacy side of things. We're talking about a fundamental right here, which says that individuals have a right to control the information that's collected about them. That's apparent to some extent in our constitution, in our jurisprudence. If I feel information about me is being inappropriately shared by government and that's severely damaging my reputation, my ability to pay to access that information, to correct it or

to find out who's getting that information really should not affect my ability to exercise my rights, in my view.

**H. Long:** Well, I wasn't basically referring to a person's rights to their information. I think everybody has a right to protect their information.

**C. Bennett:** Their personal information — sure.

**H. Long:** I was just speaking more of people looking for that information.

**C. Bennett:** In terms of FOI.

**H. Long:** In terms of the FOIable part of it.

The other thing is that you mentioned.... Maybe I'm just looking for some information on how you feel about this as an academic. You mentioned earlier that different tests were done on people that could or may not be protected under freedom of information. One of the things you mentioned was drug testing.

**C. Bennett:** Yes.

**H. Long:** We know that quite often drug testings are done and it's revealed — about drugs, the condition of a person possibly on drugs. It could be on drivers for ICBC or others.

If in fact, under the provincial law, the way we deem drugs or addictions in the province of British Columbia.... If that comes under medical, I guess I have to ask the question: if the government does see it as a medical problem in the future, would that be deemed to be giving out medical information rather than just a drug test?

**C. Bennett:** It depends on the results of the test, I guess. One of the issues about drug testing is that's a privacy issue that goes beyond the statutory provisions here. There are a variety of constitutional provisions that apply in that particular case in terms of the intrusiveness of the tests, the extent to which you can do random drug testing, etc., — the extent to which you must have probable cause before you do a drug test on an employee, for example.

I gave that example simply as one of the many ways in which personal information is collected about individuals these days. To some extent that has been going on for a long time, but it's certainly one of the more sensitive of the privacy issues that we're dealing with. The justifications for drug testing — particularly in the employment context, in my view — need to be made very, very clear and very strongly.

**H. Long:** Even if they do come under the medical information.

**C. Bennett:** Well, it's sensitive information. It's sensitive personal information in that regard. With very



few exceptions, in my view, that requires explicit informed consent of the individual concerned.

**H. Long:** Thank you.

**M. Hunter (Deputy Chair):** Thanks, Dr. Bennett, for your helpful comments. I wanted to canvass this privacy impact assessment with you again.

I think you answered. Jeff Bray put the question slightly differently. I just want to express the same concern that he did about another bureaucratic step, because I in another life was a bureaucrat dealing with regulatory impact assessments. What is intended to be a helpful service or check on bureaucratic power or service to the public — Jeff's absolutely right — can very quickly become just a checklist or something that is meaningless.

I'm very hesitant on this issue, because I much prefer what I think you put forward as an alternative, and you're not the first person to counsel us this way — that we've really got to create a culture that thinks "privacy first." I do support that.

Just a specific question on this. You say in your document that PIAs are now a standard feature of most privacy protection regimes.

[1245]

**C. Bennett:** Yes.

**M. Hunter (Deputy Chair):** You and others have said to us that the privacy provisions of PIPA are something that we should be looking at moving FOIPPA toward. Do PIAs occur in PIPA as well?

**C. Bennett:** I'm not entirely sure whether it's mentioned explicitly. Can you help me on that?

Interjection.

**C. Bennett:** It's not, no. It's not mentioned explicitly, although it is something that in PIPA's case in relation to business.... A business that's introducing a service or a product may be advised, if not mandated, by their lawyers, their consultants or the privacy commissioner to think very, very seriously about privacy protection before they introduce a new technology, a new practice, a new service, etc., because it's good business practice, not necessarily because it's a bureaucratic requirement. I think I'm saying the same thing in the public sector as well. It just makes sense to avoid the possible disasters that can occur when intrusive forms are put on the website, when hard drives end up in garbage dumps, etc. It ultimately can save money in terms of fixing the problem after the fact and reducing the number of complaints that might arise as a result of that privacy disaster.

**M. Hunter (Deputy Chair):** Thank you for that.

**B. Lekstrom (Chair):** All right. I see no further questions from members of the committee. I would like to thank you again, Dr. Bennett, for coming out and giving us your views of the act and ideas on what

could be enhanced to make it work better for British Columbians. Again, thank you very much.

**C. Bennett:** Thank you very much. I appreciate it.

**B. Lekstrom (Chair):** All right.

**J. MacPhail:** Mr. Chair, do we have a moment?

**B. Lekstrom (Chair):** Yes, we do.

**J. MacPhail:** Thank you. Then I'm going to, if I may, pursue my issue about further witnesses just a bit more, please.

**B. Lekstrom (Chair):** Okay.

**J. MacPhail:** Dr. Bennett addressed the issue a little bit about this being of concern, but I want to just reiterate that government has set up a brand-new system with significant investment in information technology around tracking FOI requests. Now, just let me read.... I can either do it here, or I can do it in the Legislature, but this is the committee where we're supposed to look at these things. Let me read about what the results of what that Atkinson Fellowship in Public Policy investigation uncovered. It uncovered:

"...massive surveillance and interference in federal access to information requests and in Ontario freedom-of-information requests for records that governments fear will lead to bad press and embarrassing questions from the opposition.

"The covert surveillance, known federally by such code names as 'Amber Light' and in Ontario as 'contentious issues management,' are run by communications advisers and strategists working for top elected officials, including the Prime Minister, the Premier and their cabinet ministers."

This is from the *Toronto Star* on November 2, 2003:

"High-priced spin doctors and political advisers, who have no legitimate role to play in the access and freedom-of-information process, are routinely allowed to view sensitive records, to question access and FOI staff about what they intend to release and to delay release until they are satisfied that they have identified all troublesome issues and prepared their political masters with the soothing public response.

"While it would be naïve to think that politicians do not monitor contentious access and FOI requests, the Atkinson investigation has shown that current surveillance systems interfere with the process. This surveillance is delaying and even preventing the release of records that we are legally entitled to receive."

That's the *Toronto Star* view of things from that Atkinson study.

It then goes on to report that some memos.... This is from September 2003 in the *Toronto Star*:

"Memos obtained under the FOI Act show that the Ministry of Natural Resources bowed to pressure from other ministries to seek an extension it did not need. The names of people making the requests for information were also revealed when they should have been kept confidential."

[1250]

Again, this is September 20 from the *Toronto Star*:

"All FOI requests from the media, members of opposition parties and anyone else who might use the records to hold government accountable for its actions and decisions are diverted into the contentious issues process. The contentious issues management system is controlled and directed by the office of the Premier and cabinet office, which is notified by ministries of all contentious requests and of the sensitive government issues contained in the records to be released. Politicians and communications advisers who have no legitimate role to play in the FOI process view sensitive records, query ministry information coordinators about what they intend to release, and often delay release until they have readied soothing public responses to thorny political issues."

That's the system that was examined in Ontario and in the federal government, and this system has been replicated here in British Columbia with a huge investment in high-tech. That's what was outlined in the Alasdair Roberts' report about the new corporate request tracking system developed by EDS, and where the Ministry of Management Services has established the corporate privacy and information access branch.

He found that they're ranked according to sensitivity, that media and opposition parties' requests are virtually always ranked as highly sensitive, and that the time to process those requests is at least double any other request. It also says in his report that this central tracking issues management group changes the sensitivity level rating of many requests from what the ministry would rank them.

I'm just saying that the changes that have occurred in the management of information requests under this government require us to look further into these two reports. I'm suggesting on that basis that we ask Ann Rees, who is a British Columbia reporter, to come and explain her research. It was a legitimate fellowship that she received in public policy. I'm also suggesting that we hook up in some way with Alasdair Roberts, who is an expert in this area and is now at Syracuse University.

I think this is a very, very contentious and very serious issue that we're exploring here. I also would suggest that the government has not in any way made public this system that they have in place either through their performance measures, their service plan in this ministry or their budget reporting. In fact, it required an FOI request to even reveal that this system exists. The FOI request was answered, but it has not been made public by the government at all.

I'm suggesting we ask those two witnesses to appear.

**B. Lekstrom (Chair):** Okay. The one thing I will point out in just having a very few moments to review it... I believe the Ann Rees issue that you speak to does not refer to British Columbia in any of her documents. When I look at this, what you've read in was not referring to British Columbia, and I want to make that very clear.

**J. MacPhail:** No, what I said was that it refers to Ontario and the federal system, but British Columbia

has replicated that system here — both those systems — unbeknownst to the majority of us...

**B. Lekstrom (Chair):** Okay.

**J. MacPhail:** ...so the tracking system of sensitivity ratings has been replicated here, newly, with a huge investment of IT.

**B. Lekstrom (Chair):** What I would possibly recommend, for the consideration of the committee, is that we have the ministry responsible come and address the committee on the very issue that you have spoken about and the issues that have arisen before the committee.

**J. MacPhail:** I'd be fine with that, but I want some.... I'm happy to have the ministry, but why not have those that have examined the ministry actions? I mean, the ministry has kept this secret, so why not have Alasdair Roberts and the ministry come? Or why not have Ann Rees and the ministry come?

**B. Lekstrom (Chair):** Okay. I do have speakers. I have Harold and then Mike, and I'll go to Harold now.

**H. Long:** I believe I haven't seen the studies that the member has brought to our attention and some of the information that she is reading from and presenting at this meeting here today. If that information could be made available to us, I'd appreciate it.

**J. MacPhail:** Sure. Absolutely.

**H. Long:** I mean, it's very hard to speak to something when only one person on the committee has that information. According to the Chair, it had nothing to do originally with B.C., but I think it was Ontario that you were speaking....

**J. MacPhail:** No, no. The report from Alasdair Roberts is about the British Columbia system.

[1255]

**B. Lekstrom (Chair):** Just for clarification, members were e-mailed the Alasdair Roberts report last week. I do have hard copies for us today that I will hand out. What I was referring to was Ann Rees, and what was read in was not reflective of British Columbia but reflective, as Joy had indicated, of Ontario. I believe even in Alberta there are articles dealing with the issues under her research. I wanted to make that very clear. Interpretation could very much be that what was read was referring to British Columbia when in fact it wasn't at this point.

**M. Hunter (Deputy Chair):** I'm not impressed by the *Toronto Star* nor much other Toronto media, to be

honest. I think the inference that the member for Vancouver-Hastings put on this is unfortunate, and I thank you for your clarification.

I think that while....

**J. MacPhail:** Mr. Chair, I object. I read into the record that it was from Ontario and the federal government. I read it right out of the article. I didn't infer at all.

**B. Lekstrom (Chair):** We will bring this back to order, Ms. MacPhail, and go back to Mike Hunter, who has the floor at this time. Thank you.

**M. Hunter (Deputy Chair):** I recognize that the member has said that this is contentious and serious in her view. I would like to suggest that we look at whether or not these operational considerations that the member brought forward have anything to do with the terms of reference of this committee, which is to review the FOIPPA and to see whether or not we're going to recommend changes to legislation. Legislative issues are not operational issues, and I think that the member's request.... I understand why she's making it, but I don't think I can agree to it.

**B. Lekstrom (Chair):** Is there any other discussion?

As the Chair, I could actually review, under the terms of reference, whether this would fit. I think it would be appropriate to have the ministry come. At the next meeting, if it was felt that it does fit under our terms of reference, an invitation to one of the two people mentioned could be discussed at that point and put on the floor for discussion.

I do have two further speakers. I will go to Sheila Orr and then Jeff Bray.

**S. Orr:** I'm just looking at the committee mandate right now, and I think it would be very reasonable to at least have the ministry here to do a presentation. I think we should review what our other member said and put it out for discussion.

**J. Bray:** I was going to concur with your suggestion on having the ministry.... We have the Alasdair Roberts reports, so I'm not sure we need to have him appear to repeat it.

The other individual's views were made of another jurisdiction. It's certainly interesting, but I'm not sure that it would be germane to have her extrapolate, necessarily, her opinion on what she observed in another jurisdiction with here. But I think having the ministry here is not an unreasonable request, and we have the Roberts report here, which we can all now go into with more detail prior to that meeting.

**B. Lekstrom (Chair):** Thank you.

**J. MacPhail:** Well, Mr. Chair, if we're going to have the ministry, then I want the minister, not the

ministry bureaucrats. I want the minister here. The minister is responsible for this. It is the aspects of the manipulation by a brand-new computer system that are being raised not only by Alasdair Roberts but by Ann Rees examining identical systems in other jurisdictions.

Why is this important? Why is it the purview of this committee? Because I'm going to recommend in our report that we institute, recommend, an amendment to the legislation that all requests for information be considered equal under the law — not delayed by double the time because it comes from a political party or the media. That's why I'm asking that this matter be put forward now.

**B. Lekstrom (Chair):** As the Chair, what I will do is.... Certainly, I have no problem extending an invitation on behalf of the committee to the minister to come and address the committee, as he's the minister responsible. I'm sure he will have staff with him at that time to help address questions.

**J. MacPhail:** She.

**B. Lekstrom (Chair):** She, at this point — yes, because of the changes.

What I would like to do is with the information that has been put before you, handed out, on the Alasdair Roberts report.... Rather than debate what I think is probably somewhat premature, the contents of that report, I would encourage the members of the committee to go through that and at our next meeting raise that issue again. I think it would be more productive for each member of the committee as well as the committee as a whole to address that matter in this manner.

**J. MacPhail:** I'd be happy to make available what I was reading from — despite the member's views on the *Toronto Star*. I'd be happy to make that available too.

[1300]

**B. Lekstrom (Chair):** Very much appreciated. Thank you.

With that, we will move on to our next presenter here today, followed at the end of that by any other business on the agenda.

I will call on Mr. Ted Hayes to come forward and make a presentation to the committee. Good afternoon, Mr. Hayes.

**T. Hayes:** Good afternoon, Mr. Chair, hon. members and guests. I have a written presentation, but my oral presentation will vary somewhat from it. The conclusions are the same, but some of the facts that I introduce are a little different and the order of presentation is different. I don't think you have the written submission at this time, in any event.

My purpose here is to give a critical examination of the act from my own experience. I don't think the act is working very well, although I recognize the work of the people who framed it and the people who implemented it, and I think they did it with the best will and intentions. I think there are a lot of changes that need to be made to make this process work better.

Now I'll tell you some stories. In 1991, I started researching a paper, which was based largely on government mental health statistics. I published the paper in an international journal. The statistics that I received from the ministry at that time were computer generated. The results that I got from this were that due to the quality-control mechanisms the government had implemented — and this was largely to do with computers — the cost of running the service had gone up, but the quality of the service had gone down.

I should perhaps add that parenthetically, the costs and benefits of the processes of quality control might still be in fact reducing the quality of the service and increasing the cost. I refer to things like accreditation, which are going on right now, that are very costly and perhaps have doubtful value.

In 1996, I decided that I wanted to update the research figures that I got in 1991. As you'll recognize, 1991 was before the act was passed. At that time the Ministry of Health denied that any such figures existed. I applied to the office of information and privacy. They mediated the situation. The Ministry of Health eventually found that they did have the statistics, but they didn't have them in computer form. I don't know why they would have had them in 1991 and not have had them in 1996. It just doesn't make any sense to me. They said that they only had handwritten paper copies of the information I wanted.

The process took months and months and months to go through, and at the end of it they wanted hundreds of dollars from me in order to get the information that I had previously got for free before the act. So in 1991, I got information without the act. In 1996, I didn't get the information that I wanted, and it cost me a great deal of money. I think one of the conclusions that I am drawing from this is that in many cases information may be more difficult and costly to obtain since the Freedom of Information Act.

In 1978 — that's a long time ago, but I'm old enough to have worked at that time — I requested some information on compulsory admissions to mental hospitals and psychiatric facilities in the province. I got it. It took me six months to get it. It took me a lot of letters, including a letter to the minister, but I did get the information. At the time I was particularly outraged. I thought it was outrageous that I should have to wait six months to get information. One has to understand that this is the revocation of what are now people's constitutional and certainly their civil rights. Nobody was keeping a record of it, and when I asked, they actually had to go round and find out. But they did, to give them credit at the time. As I say, I was outraged at the time. I did get the same information from

other provinces at that time, and from the United Kingdom. I was living right here in B.C.

[1305]

In 2002 we've got a Charter of Rights and Freedom, we've got the Freedom of Information and Protection of Privacy Act, and things are worse. I began in 2002 by informally requesting from the Ministry of Health information about compulsory admissions. I was also interested in some security information, but compulsory admissions are germane to this because I had asked for the same thing in 1978. Nobody replied. I applied to all the health authorities, and nobody replied. I repeated the request again after two weeks. Two of the authorities replied. One of them actually delivered, subsequently; the other one didn't. The one that delivered was the provincial health services authority.

So I made a freedom-of-information request. It took me five months to get the information that I wanted on security — that is, the level of security that was being applied to people who were being held — but I got data on compulsory admissions from most of the authorities. I didn't get it from the interior health authority. I didn't get it from the Vancouver coastal health authority. I didn't get it from the northern health authority, and as you may or may not be aware, the northern health authority is the authority in which I live.

By December 2002–January 2003, I hadn't received any information, and I was advised that I might try the Ministry of Health. I already knew that the health authorities were obliged to gather that information for the Ministry of Health. I knew they had it, but the Ministry of Health itself might have this. Again I made some information requests to the Ministry of Health. They didn't answer me. When they did answer me, I was told that the information didn't exist.

I knew where the information was located, so I told them at the Ministry of Health where in their ministry it was located — because nobody seemed to know, or they said they didn't know. They went through a number of undertakings to provide the information. There was some correspondence back and forth between me and them, with me saying, "What's happening?" and them saying: "We're just about finished." That ceased about six months ago, and I have heard nothing since.

In that same time I received equivalent information from 75 different governments and authorities, many of them outside Canada. From the United Kingdom and the government of Saskatchewan I received the information almost by turnaround. When I had follow-up questions, they were answered immediately. But in British Columbia I couldn't get the information. It's a year and a half later; I still haven't got it. The collection and storage of information may have deteriorated in the last decade or two or three perhaps, and it may be more difficult to obtain. Information is easier to get from other governments.

My interests are in public policy. I'm just an ordinary citizen; I don't represent anybody. But I do have

an interest in public policy, and as you can see, I am particularly interested in mental health policy — but not exclusively, and I'll raise some other issues later.

[1310]

In 2002 I became concerned that contractors were progressively being used more and more in the public service to do the work of public servants. I was concerned that that might raise problems for the public for a couple of reasons. One is that the level of accountability was different, and members of the public dealing with contractors, believing them to be members of the government service, wouldn't necessarily know they weren't getting the same level of accountability. Also, there were issues about conflict of interest, and I felt that issues of conflict of interest were more prevalent with contractors or could potentially be more prevalent with contractors because they weren't governed by the rules that govern the public service. Those are fairly specific, fairly extensive, and I don't have any problems with them. But contractors who may be working within the public service — as public servants, ostensibly — aren't necessarily governed by the same thing.

I originally raised that issue with the merit commissioner. I went and talked to him. I told him about what I saw to be the problem and some examples of where I saw the problem existing, simply as examples. He said it wasn't within his mandate to deal with that kind of thing but that I should perhaps take the examples up with the ministries that were relevant, and then I could see where I could take it from there. I duly did that.

The first area I went to was the Ministry of Health. One of the examples I was using was actually from the provincial health services authority. As you can understand, at that time it was sort of just being developed. I was aware of a contractor, who I subsequently learned was a subcontractor, who appeared to be in some kind of conflict of interest. It provided an example of what I was saying.

The public health services authority denied that there were any potential or actual conflicts involved. It meant that I had to get the contract in order to see this particular conflict. I made an FOI request, but I was denied the contract. They sent me a whole sheaf of papers. I mean, they can't be faulted for volume. Relevance was a really big problem, though. They didn't seem to have very much to do with what I'd asked.

The FOI process started proceeding. That is, we went through the time limits and everything, and they extended and did all the stuff they did. Then it started to come up for review, and as the review went on....

Now, I should explain this. You perhaps are aware that as soon as a review starts, the lawyers get involved. I'm the citizen, but I'm not dealing with a public service agency, any public body, anymore. I'm dealing with a lawyer. In this case it was an independent lawyer, but it's irrelevant, I guess. As this process went through the review, they started giving me more and more of the papers I had asked for. I still haven't got them all, and it is a couple of years later, but they did start to give them to me.

As they gave them to me, it became more and more evident that what was happening was that there was no written contract. I'd asked for a contract, but there wasn't one. Obviously, as I'm sure the members are aware, to form a contract, you don't have to have anything written, but it's certainly not a prudent method of going about business.

There was no contract. Then it became evident that there was about a quarter of a million dollars spent. Then it became evident that there was no request for proposals either. Then it became evident why it was that they hadn't given me the information in the first place.

I feel concerned that the FOI.... I know my way around a little bit. I know the way government works a little bit. I can speak to a special committee of the House, but most people can't. I think most people making ordinary requests of the government for information wouldn't pursue it in the way I happen to be. People say I'm a bulldog. Maybe I am, but this is what's happened. You have to be a bulldog in order to get it.

As I say, this process is still before the commissioner, but I have got most of the papers, and I can tell you with some degree of assurance that the information I have given you is true and correct. That is, the conclusions I have given you are true and correct.

[1315]

There was another aspect to this thing. Where there were documents — and there were certainly some documents that concerned this particular contract — what also became evident was that most of the work the contractor had contracted for. Where the subcontractor was doing most of the work, the subcontractor was not doing work that had ever been described.

The contractor was actually doing a public service job. He had a government business card. He had a government office. He had a government telephone. He had a government e-mail. For all intents and purposes, he was a government person, and he was a government person working in a supervisory capacity. That was also evident. I'm told he went through disciplinary processes with employees. None of this was ever described in any of the documents I got.

As I say, I think there is a serious problem when this doesn't easily become evident. I am aware that people will try and cover when there are idiosyncrasies going on, when there are problems, but I think there could be a serious problem here. Despite the FOI Act, I think public bodies may still withhold information that's damaging and embarrassing. I think the public bodies may depend on processes that are lengthy, laborious and legalistic in order to deter citizens from pursuing information that may be damaging, embarrassing or otherwise inconvenient.

The final example I want to give you is one that's perhaps a little bit more politically loaded than the others. I should be clear that the information that I've given you so far, as I'm sure you're aware, isn't confined to any particular government. It's a systemic problem. In 2001, I applied for the incomplete report

that was made by Murray Smith on gaming and the Nanaimo Commonwealth Holding Society. The Attorney General called a halt to that inquiry in June, and I applied for the unpublished report seven days afterward. I heard Murray Smith on the radio saying that it was 85 percent written, and I thought that as I had paid for it, maybe I should be able to read it.

When I applied to the Attorney General's office, they immediately replied, which is quite unusual in my experience. It may sound otherwise, but I've only actually made about a dozen inquiries over the life of the act. They don't usually turn around requests right away. I got this one the next day. They said they didn't have it, they didn't know where it was and they didn't know anything about it. Their minister had issued a press release on it only a week before.

I applied to FOI for that. Eventually the mediator told me he wasn't getting anywhere with the Attorney General and that I should apply to the Gaming Commission. So I applied to the Gaming Commission, only there wasn't one. They had been sucked into the Solicitor General's ministry, so I applied to the Solicitor General. But it turns out that the Solicitor General doesn't deal with their own FOI inquiries. Attorney General does, so I was back with the Attorney General.

A little while later I got a letter from the Attorney General to say they had passed the information to the B.C. Archives and that I would have to go to B.C. Archives to get it. I contacted B.C. Archives, and after 30 days B.C. Archives asked for a 30-day extension because they wanted to consult with the Attorney General. B.C. Archives refused the application eventually, after 60 days. Of course, this is not 60 days. This is three months, because it's 30 working days plus 30 working days, which in my mind is not 60 days.

[1320]

I appealed the B.C. Archives application, and of course B.C. Archives was represented by the Attorney General. We went to review, and I won the review. I won it in spite of the fact that it was me against the lawyers of the Attorney General. At the end of 30 days — because they're required to give it up within 30 days — I received notice from the Attorney General that the Attorney General was going to take the information and privacy commissioner to court, and I'm named in this action. So I, too, am being taken to court.

Not only am I being taken to court by the Attorney General, but it turns out that there are a whole bunch of other people who want to take the FOI commissioner to court, and they're taking me to court too. And I have good reason to believe that all or most of them are having their legal fees paid by the Attorney General, but I'm not. Here we are with me jammed in between two levels of government because I asked for some information. I'm being jammed into a court case that I didn't ask for. I just asked for information. If I had lost this case, I suspect I wouldn't be there, but I'm there now. Quite frankly, I just don't think that's fair.

I think there need to be some changes here. The irony of this whole thing is that we've got one arm of

the government taking the other arm of the government to court. The FOI commission has had its money cut by the Legislature, so it's got less money, but now it's having to put out more money in order to keep this case going. I mean, I'm glad that they're not backing off on the case, but nonetheless it's costing the commissioner money that is actually less plentiful now than it was.

For my money, that's an unacceptable situation. Even if I win — again, I'm assuming that you know, but I'm going to go through this just the same — and I do get this information, the Attorney General or the B.C. Archives or whoever it is will be ordered to give me the documents. That doesn't mean to say that they can't excise them, and that doesn't mean to say, if it's 200 pages, that I'm going to get 200 pages with "page 1" written on the first page and "page 2" written on the second page and that's it. Then I'm going to have to go back to the FOI commission, if I really want to see this document, and go through the whole damn review process all over again. This is going to take months and months, if not years and years, to resolve, and I don't think that's a worthwhile expenditure of government funds. I don't think it's a just kind of freedom of information, and I don't think it leads to freedom of information.

How am I doing? Oh, I'm really overextending my time. I have some recommendations. I did write them in my written submission, which you will get, and they are related to what I have said. I mean, I won't bother at this time, but I will read the conclusion that I've written.

I think the act has unwittingly created a bureaucratic and legalistic process that is not easily accessible to ordinary citizens. The public bodies may still withhold embarrassing or damaging information in the hope that the citizen will be the first to give in, and I suspect they have been, in many cases that we don't even know about. I don't think it's acceptable that governments in other provinces and other countries may be more readily providing information to the citizens of this province than the citizens' own government.

I think the prospect that as a result of a request for information, a citizen may find himself or herself in court will do little to quell the freeze of government information, and that one arm of government should pit itself in court against another arm of government simply can't be tolerated. If it were, for example, that the treasury decided they were going to cut the ministry by a certain amount, the ministry wouldn't take the treasury to court because it didn't give it enough money, even if it were unjust. But they appear willing to take the office of information and privacy to court. The Legislature has already cut the expenditures of the commissioner, and now the machinery of government is forcing more litigation expenses on it.

[1325]

It appears to me that what's required is not less freedom of information. It's a stronger office of information and privacy. I think that can't be accomplished unless there are greater powers and greater resources allocated to it, and that's what I recommend.

Thank you.

**B. Lekstrom (Chair):** Well, Mr. Hayes, I want to thank you for taking the time and the effort to come and see us. I know that originally we were scheduled to come to you. Unfortunately, that didn't work out, so I do appreciate the effort that you've put in.

**T. Hayes:** My home is always open.

**B. Lekstrom (Chair):** All right. I want to look to members of the committee if they have any questions.

**B. Penner:** Mr. Hayes, thank you for your presentation. I actually had the chance to read your 11-page brief.

**T. Hayes:** Oh, thank you.

**B. Penner:** I appreciate you giving that to me.

Just a question. The other parties that you say are involved in this case — this is involving the Bingogate or the Nanaimo Commonwealth Holding Society — do you know who those other entities or parties are to this reported litigation?

**T. Hayes:** I can tell you more than that. I don't have any relationship to any of them. I don't have any relationship to gaming. I don't have any information on the Nanaimo Commonwealth Holding Society. I don't have any relation to any of that stuff. I want to make that clear to begin with.

I don't know these people. I know one name. One name is the name of a former Attorney General of the province; another name, I understand, is his executive assistant. I think some or all of the rest of the people may have been public servants, but I don't know them, and I don't know for sure.

**B. Penner:** So they have all joined in this effort to overturn the decision of the commission to release the information?

**T. Hayes:** Yeah. So they've all mounted their separate cases. I guess there must be nine cases, but they're all kind of conjoined. I actually asked the Attorney General, because I wanted to know for sure who was being paid by the Attorney General. But when I made a freedom-of-information request, the Attorney General wouldn't give me that information.

I'm not going to appeal it, I don't think. There's no point. I just wanted to know. But I have reason to believe that the lawyers are being paid for by the state.

**B. Penner:** When is the hearing going to be to determine whether this information will be released or not?

**T. Hayes:** Oh, it hasn't got anywhere near that yet. There is a meeting this month to decide how they're

going to proceed. It's so complicated now, because there's so many people involved, they have to have a meeting now with a judge in chambers to decide.... I've forgotten what it's called. Case management is what it is. They are deciding how this case is going to be managed — who is going to say what and why they are going to be saying it, and that kind of thing.

It looks to me like it will be.... I think they're suggesting that it might go to court in April, but who knows?

**B. Penner:** I'm casting my mind back a ways to try and remember all the parties that were involved during the commission hearings, but it sounds to me that the people who were involved in that commission process — hiring lawyers and so forth — may well be the same people here.

**T. Hayes:** I think they are — yeah, probably.

**B. Lekstrom (Chair):** I'm going to look to other members of the committee if they have any questions to Mr. Hayes this afternoon.

Mr. Hayes, I see no further questions. I do want to thank you again for taking the time and effort to come and address the committee. As all other presenters and written submissions that this committee will review, I can assure you that you will be given due consideration in the presentation of our report and development.

**T. Hayes:** Thank you. For me, this is a bit of a catharsis. I've been getting pissed off for a long time.

**B. Lekstrom (Chair):** Hopefully, we can help you correct that.

That concludes the witnesses to present before the committee this afternoon. We will move on to item 3 on our agenda, which is other business.

[1330]

#### Other Business

**B. Lekstrom (Chair):** I will bring up the issue that should the committee wish to meet, we will have to do it before February 10, at which time I understand our committee will be defunct until it is recommissioned through the Legislative Assembly.

We do have some work to do, and I anticipate the committee will be put back together. Would it be the wish of the committee to try and accommodate a meeting prior to the beginning of the sitting of the Legislature? A recommendation I could put forward would be Monday, February 9 in the afternoon, hopefully, to hear from the minister responsible at that time as well as discuss where the committee goes from here in the development of our report and see if we have the information needed to begin deliberations for that report.

I will look to members.

**J. MacPhail:** Mr. Chair, fine. But are you going to attempt to at least ask one of these other witnesses to

come forward, or both of them? I don't understand why we're going to give the minister say and not.... That's antithetical to the point that I've been raising. Anyway, I leave it with you, Mr. Chair, to fulfil my request that if the minister comes forward, we have — at a minimum — Ann Rees or Alasdair Roberts present to us, or both.

**B. Lekstrom (Chair):** I will take that under consideration. I am going to spend some time, like all of you, I'm sure.... Under the terms of reference, I'm not sure ours is to guide the administrative process of this but to review the act. I want to make sure that what we do as a committee follows the terms of reference that the Legislative Assembly set for us and that were adopted.

**J. MacPhail:** And if the act is not treating everybody equally under the law, then we need to change the act, and that's why I raised the point.

**B. Lekstrom (Chair):** Correct. I think my interpretation of the direction that I'm going to plan on taking would be to have the minister here first. At that time, once that information.... We're talking about the rating system that you have raised. If the committee wishes — it will not be my decision solely; it will be the decision of this committee — to extend an invitation to either of the parties or both of the parties you've raised....

Now, there are many meetings set up for the 9th of February, and I'm sure there are committee members who will sit on each of them. I will try and accommodate this on Monday, February 9 throughout the day. I will get the information to you and hopefully, as quickly as you can, respond to try and accommodate this meeting. That would be very much appreciated.

**J. MacPhail:** What are the other committee meetings, if you wouldn't mind? There's Public Accounts, I know.

**B. Lekstrom (Chair):** Public Accounts is that day. Crown Corporations meets from one until two. So even if we met following 2 p.m., I think it may work. I'll get that information out to everybody. Okay?

Is there any other business to be brought before the committee this afternoon?

Seeing none, just before closing, there is interest in the written submissions from the public wanting access. I felt it was appropriate that we make sure each committee member has those written submissions prior to releasing those to the public per se. We hope to have all of those in your hands in the near future, as well as a briefing or an overview of the submissions presented to the committee so far. If that's acceptable, I would look for your approval on that. In the past I believe it's been handled in different ways. A written submission to the committee is, I think, a public document. Out of courtesy to the committee, I think it's important that we receive those first and then make them fully available to the public upon request.

**M. Hunter (Deputy Chair):** How many written submissions have we received so far? We've still got 28 days or so — right?

**B. Lekstrom (Chair):** I believe 20 is the number, approximately, so far. The written submission deadline, I believe, is the 27th of February, so we do have a considerable amount of time, and I assume we will receive a significant number of submissions yet.

With that, a motion to adjourn would be in order.

The committee adjourned at 1:34 p.m.