Legislative Assembly of Alberta

The 27th Legislature
Third Session

Standing Committee on Health

Freedom of Information and Protection of Privacy Act Review

Officers of the Legislative Assembly and Public Presentations

Thursday, September 2, 2010
9:02 a.m.

Transcript No. 27-3-8

Legislative Assembly of Alberta
The 27th Legislature
Third Session

Standing Committee on Health

McFarland, Barry, Little Bow (PC), Chair
Pastoor, Bridget Brennan, Lethbridge-East (AL), Deputy Chair

Blakeman, Laurie, Edmonton-Centre (AL)*
Elniski, Doug, Edmonton-Calder (PC)**
Forsyth, Heather, Calgary-Fish Creek (WA)
Groeneveld, George, Highwood (PC)
Horne, Fred, Edmonton-Rutherford (PC)
Lindsay, Fred, Stony Plain (PC)
Notley, Rachel, Edmonton-Strathcona (ND)
Olson, Verlyn, QC, Wetaskiwin-Camrose (PC)
Quest, Dave, Strathcona (PC)
Sherman, Dr. Raj, Edmonton-Meadowlark (PC)
Taft, Dr. Kevin, Edmonton-Riverview (AL)
Vandermeer, Tony, Edmonton-Beverly-Clareview (PC)

* substitution for Kevin Taft
** substitution for Fred Horne

Department of Service Alberta Participant

Hilary Lynas	Director, Access and Privacy

Office of the Auditor General Participant

Kerry Langford	General Counsel

Office of the Ethics Commissioner Participant

Brad Odsen, QC	Registrar, Lobbyists Act, and General Counsel

Office of the Information and Privacy Commissioner Participant

Marylin Mun	Assistant Commissioner

Support Staff

W.J. David McNeil	Clerk
Louise J. Kamuchik	Clerk Assistant/Director of House Services
Micheline S. Gravel	Clerk of *Journals*/Table Research
Robert H. Reynolds, QC	Law Clerk/Director of Interparliamentary Relations
Shannon Dean	Senior Parliamentary Counsel/Clerk of Committees
Corinne Dacyshyn	Committee Clerk
Jody Rempel	Committee Clerk
Karen Sawchuk	Committee Clerk
Rhonda Sorensen	Manager of Corporate Communications and Broadcast Services
Melanie Friesacher	Communications Consultant
Tracey Sales	Communications Consultant
Philip Massolin	Committee Research Co-ordinator
Stephanie LeBlanc	Legal Research Officer
Diana Staley	Research Officer
Rachel Stein	Research Officer
Liz Sim	Managing Editor of *Alberta Hansard*

Transcript produced by *Alberta Hansard*

Standing Committee on Health

Participants

9:02 a.m. Thursday, September 2, 2010

[Mr. McFarland in the chair]

The Chair: Well, good morning, everyone. Welcome back on the second day of September. Everyone is happy to be here, I'm sure. I know Ms Blakeman is. She's looking forward to a whole day of FOIP review. To those that are on the air listening in, welcome.

I think we'll start the morning, as we normally do, with an introduction of ourselves for the record. If I could start on my immediate left with our committee clerk.

Mrs. Sawchuk: Karen Sawchuk, committee clerk.

Mr. Quest: Good morning. Dave Quest, MLA, Strathcona.

Mr. Olson: Good morning. Verlyn Olson, Wetaskiwin-Camrose.

Dr. Massolin: Good morning. Philip Massolin, committee research co-ordinator and table officer, Legislative Assembly Office.

Ms LeBlanc: Stephanie LeBlanc, legal research officer, Legislative Assembly Office.

Ms Lynas: Hilary Lynas, Service Alberta.

Ms Mun: Marylin Mun, office of the Information and Privacy Commissioner.

Ms Blakeman: Laurie Blakeman. I'd like to welcome each and every one of you to my fabulous, still summerlike constituency of Edmonton-Centre.

Mr. Vandermeer: Good morning. Tony Vandermeer, Edmonton-Beverly-Clareview.

Mr. Groeneveld: George Groeneveld, Highwood.

Mr. Lindsay: Good morning. Fred Lindsay, Stony Plain.

Mr. Elniski: Good morning. Doug Elniski, the MLA for Edmonton-Calder, substituting for Fred Horne.

Ms Pastoor: Good morning. Bridget Pastoor, Lethbridge-East and deputy chair.

The Chair: I'm Barry McFarland, chair, from Little Bow.

Mrs. Forsyth: I'm Heather Forsyth.

The Chair: Good morning, Heather.

Mrs. Forsyth: Good morning.

The Chair: Anyone else?

Ms Blakeman: Sorry, Mr. Chair. I forgot to mention that I'm substituting somewhat permanently for Dr. Taft.

The Chair: Thank you, Ms Blakeman.

Members now have probably received the revised meeting agenda and the supporting documents. They have been updated, and they were posted to the internal committee website. If anyone needs copies of the meeting materials – I don't see anyone with a hand up – they are available.

Okay. Any additional items that anyone needs to have added to the agenda? Seeing none, could we have a motion to approve the agenda as circulated for today's meeting of the Standing Committee on Health? Mr. Olson. All in favour? That's carried. Just for the record we don't need to have a seconder for any of these motions.

Our future meeting dates. We currently have September 13 and 14 booked as review dates from 9 till noon each day and October 28 shown as the date for the review of our draft report. Now that we're further along in the process, I'd like to suggest that we look at how to balance the review and how it may unfold considering the revision of and adding or changing some of the meeting dates. Because of the research component to it I'd like to suggest that we move the September 13 and 14 dates to September 27 and have one day from 9:30 in the morning to 4 p.m. to review all the recommendations and to decide which of these recommendations the committee wishes to put forward on the final date.

By way of explanation, then, I could say that this would give our research staff time to compile all the requested research and have this information for posting the week prior to the meeting. Currently we wouldn't be able to do that with September 13 and 14 because there are only four business days after we complete our meeting tomorrow, and this would likely not provide sufficient time for the work to be completed and circulated, as is required, in advance of the meeting dates.

Ms Blakeman: Where does the chair anticipate the recommendations will come from if we don't meet between the end of seeing the presenters and deciding and debating which recommendations will go forward? I anticipated that we'd be meeting to develop those recommendations, to go through and say that these are the ones that we want to discuss, and then come back and discuss them. Who's going to be developing these recommendations?

The Chair: Could I ask Dr. Massolin to give us a hand here with this, please?

Dr. Massolin: Yes. I can just speak to the issue, I guess, of the lead time that might be required, depending on what the committee asks for. I think, if I can say, the chair was asking for a little bit more lead time for our research staff to prepare requested documents; for instance, perhaps a summary of not only the information that the committee has received to this point but also the information it will receive today and tomorrow so that there could be a list, basically, of the standout issues, if I can call them that. The committee at the subsequent meeting could go through those issues and deliberate on them and decide which ones. You know, in addition to the ones we present, obviously, there's an opportunity to indicate additional information as well. The idea there, I think, is just to give a little bit more lead time than has been allotted here with the 13th and 14th of September meetings.

Ms Blakeman: Yeah. I don't have a problem with giving the staff more time – that's very reasonable – but my experience on these committees is that it does take the committee a while to hash through all of the recommendations that are in front of us and make a decision as to how things are going to go forward. I would really caution against narrowing this down to one day rather than the two days that were anticipated. At one point these were two full days. Now they've turned into two half days, and now we're talking about trying to do this in one day. That's going to be really difficult just

given the complexity of what's in front of us and how important this issue is.

Thanks.

The Chair: I may be wrong about the timing, Ms Blakeman, but I do know that we had two half days scheduled. Now it'll be one full day. Maybe Karen could elaborate a little bit more if you don't mind.

Mrs. Sawchuk: Mr. Chair, I believe that just during discussions through the last few meetings the committee had set the times for those two dates, and that's when they were posted on the websites. That's what we did have on the record.

Ms Blakeman: And I probably complained at the time that going to two half days wasn't a good idea, but there we are.

Mrs. Sawchuk: That's likely it, yeah.

9:10

Mrs. Forsyth: If I may, Mr. Chair. The September 27 date does not work for me. We're in meetings all day that particular date. I just have to get that on record. Has there been something put out in regard to the rest of committee on that particular day, September 27, to see if they can attend?

The Chair: That's what we're discussing right now, Mrs. Forsyth.

Mrs. Forsyth: Okay. Thank you.

The Chair: Any other comments from anyone?

Mr. Vandermeer: You wanted the 27th and 28th, right?

The Chair: No. We're suggesting that rather than having two half days, Tony, we'd have one day, the 27th or 28th. I know there are already some other committee meetings, I believe, on the 28th.

Mr. Vandermeer: The 28th is our CPC meeting.

The Chair: Okay. I was just going to suggest that perhaps the 27th would better accommodate all the way around. I'm at the committee's will.

Ms Pastoor: The 27th isn't good for me either.

The Chair: Well, Mrs. Sawchuck has suggested that we can always look at additional meeting dates as well, but I guess the first thing we have to do is appreciate that the 13th and the 14th logistically, if somebody wants to get technical about it, don't give us enough working days to have everything posted and really wouldn't be fair to the research component, who are compiling everything. So I don't think the 13th and 14th are going to work. I guess that's what I'm trying to get out on behalf of the clerk and the research people.

Could we deal with that in terms of: are we in agreement that we should find another day to begin with? Okay. Now, whether or not it's going to be the 27th, the 28th, or some other date, I'm open to suggestions, please.

Mr. Groeneveld: Mr. Chairman, I see that this room that we're in right now is occupied on the 28th already.

The Chair: This one?

Mr. Groeneveld: Yes.

The Chair: Okay.

Ms Pastoor: Mr. Chair, I think that so far we've only heard that it will be a problem for Mrs. Forsyth and myself. I can wiggle around my obligations on the 27th if that would help. I'm not sure about Mrs. Forsyth.

Mrs. Forsyth: No. I am booked solid on the 27th – I'm sorry – as is the rest of our caucus.

The Chair: Okay. We have Mr. Vandermeer. Then we'll have Mr. Quest.

Mr. Vandermeer: I would suggest that we go with the 27th. With all our schedules it's going to be so hard. I mean, somebody is going to always be busy. We always have replacements. So I would suggest that we go with the 27th date.

Mr. Quest: I've got one meeting on the 27th, Mr. Chair, but again I'm sure that can be rescheduled if necessary. I guess that if it's the 27th, it's the 27th if that's the will of the group.

The Chair: Ms Pastoor, is yours a timing thing? You'd suggested you could move it around.

Ms Pastoor: Yeah, I can wiggle around what I have on that date. I can do it if I really have to.

Ms Notley: I'd like to see us look at another couple of dates. I mean, this is the meeting at which we're going to talk about the recommendations of the committee, so looking at just one date when, you know, one caucus cannot be represented at that meeting seems a bit – maybe we should give it a little bit more of a try to find something to accommodate everybody.

The Chair: Yeah. We won't have a problem with that, Ms Notley. I just wanted to find one date to commence after the 13th and 14th.

Okay. While we're here, I'd like to welcome Ms Notley. She was in the door but hadn't quite gotten here when we introduced ourselves. Thank you very much.

I'm sorry, Heather. It looks like there may be a consensus for at least the one meeting for September 27 from 9:30 till 4 to take the place of the 13th and the 14th.

Mrs. Forsyth: Okay, Mr. Chair.

Ms Notley: Okay. Well, Mr. Chair, I guess that maybe I didn't make myself clear. What I was suggesting was that we see if we can throw at least one other day out there because, again, given the import of the meeting, we ought to try to ensure, beyond just throwing out one day, that we can get everybody there.

Mr. Olson: I was just going to, I guess, include my information. I'm available on the 27th, and I've been advised that Dr. Sherman is also available on the 27th. I'm wondering about the 29th. I'm also available that day, a couple of days later but the same week.

Mrs. Forsyth: Barry, if I may, the 29th doesn't work for me. The 30th doesn't work for me. Please feel free to go ahead on the 27th, and I'll see what I can do. We've got caucus meetings all that day, so I'm going to have to talk to my caucus.

The Chair: Okay. Thank you for that.

Ms Blakeman: Sorry. Was that true for her on the 29th, too?

Mrs. Forsyth: Yeah.

Ms Blakeman: Oh, sorry. Okay. The 29th works for me.

The Chair: Mr. Lindsay, please.

Mr. Lindsay: Thank you, Mr. Chairman. As a follow-up to Ms Notley's comments, I think it may be advisable to at least set another date other than the 27th. If we don't need it, that's fine, but if we run out of time on the 27th and then all of a sudden we're trying to set a date when our schedules are already filled up, this gives us a better opportunity, maybe, to get some agreement on another date in case we need it.

The Chair: Okay. The committee clerk is also looking at a schedule saying maybe also October 4 and 5.

Mrs. Forsyth: Barry, the 4th doesn't work for me, but I can do the 5th.

The Chair: The 4th doesn't?

Mrs. Forsyth: No.

The Chair: Okay.

Mrs. Forsyth: But the 5th I could probably do. I think it's important, you know – to the committee, it's up to their schedules also, not just myself as someone from the Wildrose Alliance. I will see what I can do on the 27th, but I can't commit until I speak to my caucus.

The Chair: Okay.

Mrs. Forsyth: I can do the 5th.

Ms Blakeman: Mr. Chair, that first week in October affects the Edmonton MLAs because it's Read In Week in our schools, and I know that some of the MLAs have a lot of schools. Maybe if we started now, we could organize around it. I don't know. I'm looking at Mr. Vandermeer and some of the other Edmonton people. If I start now, I can work around and keep one of those two days clear, but for people that have 30 schools . . .

The Chair: From the looks and the sounds of the comments, it appears that the 27th and the 29th are probably going to be the most doable for now. That doesn't preclude – you know, if we get bogged down, we will have to find another date. Period. Okay?

Ms Blakeman: So we're doing the 29th from when until when?

The Chair: Well, it would be, I'm going to assume, a similar time schedule.

Ms Blakeman: So 9:30?

Mrs. Sawchuk: Well, 9:30 to 4 or 9 to 4 or whatever the committee prefers.

The Chair: Okay. On the 27th from 9:30 until 4.

Mr. Groeneveld: Well, 9:30 until 1 will work for me.

The Chair: On both days or one day?

Mr. Groeneveld: No. On the 29th.

The Chair: Okay.

Mrs. Forsyth: Mr. Chair, you're so soft-spoken. You're going to need to speak up.

The Chair: I'm soft-spoken? You know me. That's a compliment.

Mrs. Forsyth: Yes, it is.

The Chair: All of us are looking up at the ceiling, wondering.

Mrs. Forsyth: If everyone could speak into the microphone because people keep fading in and out.

The Chair: Thank you for that.

So we are now, Mrs. Forsyth, on the 27th from 9:30 until 4.

Mrs. Forsyth: Correct. Yes, I have that.

The Chair: On the 29th, it may in all likelihood be scheduled from 9:30 to 4, but it might end by 1. Or it may not happen at all if we are really diligent and get the work done on the 27th.

Mrs. Forsyth: All right. Thank you.

9:20

The Chair: You're welcome.

Now that we've got that part out, I'd also like to suggest we change the timing of our date to review the draft report because of what we've already done. We currently have the morning of October 28 booked, but additional time may be required to incorporate any final changes to the committee report. Would the committee be agreeable to meeting some time earlier during the week of October 25 or moving to the week of October 18 to review the draft report? The final meeting could then be scheduled as set out in our approved timeline, some time during the first two weeks of November.

Ms Blakeman: Mr. Chair, I'd far prefer we tried to meet during that week of the 18th because once we get into session, we've got different caucuses meeting at different times, and it gets really problematic. I know that on the 28th we were meeting after session lets out, I think at 4:30. We might want to hang onto that, but I think we should move back into that week of the 18th.

The Chair: I do know that the 20th and the 21st are not good.

Ms Blakeman: Oh, the municipal election. What am I thinking?

Ms Pastoor: When is that?

The Chair: That's on the 18th.

Ms Blakeman: Yeah.

The Chair: On the 19th?

Mrs. Forsyth: I can't do the 19th, Barry.

The Chair: Okay.

Mrs. Forsyth: On the 20th we have our Heritage Savings Trust Fund meeting in Lethbridge.

The Chair: Right.

On the 21st there are meetings in Lethbridge that are unrelated to the Heritage Savings Trust Fund meeting. The 22nd? Going once.

Mrs. Forsyth: I can't do the 22nd, Barry, but I will be at the will of the committee.

The Chair: Does the 22nd not work for anyone other than Mrs. Forsyth?

Mr. Lindsay: It doesn't work for me.

The Chair: It doesn't work for you? You can find a substitute.

Mr. Lindsay: I could.

The Chair: You could.

Mr. Lindsay: I would miss being with all you fine folks.

Mr. Groeneveld: Mr. Chairman, it's going to be difficult for you and me. If you look at the schedule, we're tied up in Lethbridge on Thursday night.

Ms Blakeman: Well, maybe the meeting could be in the afternoon then. Friday afternoon. Oh, my God, that will be fun.

The Chair: I guess I'm not too sure. It comes back to the following week, and like Ms Blakeman said, then we're fresh into session.

The committee clerk has suggested this for you: could we possibly choose these dates at our next meeting?

Ms Blakeman: Uh-uh.

The Chair: You want to do it now.

Ms Blakeman: It just gets worse.

The Chair: Okay. All right. Then, I'm just begging you to help me, please, find a day.

Mrs. Forsyth: Mr. Chair, if I may. I have in my calendar October 28, which is a Thursday, as a Standing Committee on Health FOIP. Was that meeting not booked previously? It's in my BlackBerry.

The Chair: Yes, that was the date, Mrs. Forsyth, that we had booked. I think the only reason we're looking at it now is because session will have started and everyone may be rather caught up in session. The timing of having this meeting on the 28th . . .

Mrs. Forsyth: I just wanted a clarification because it's already in my calendar. October 28 works for me.

The Chair: The 28th – I'm sorry – is what day?

Mrs. Forsyth: That's a Thursday.

Ms Blakeman: Which is a short sitting day. So why can't we use that day to review? We're looking at reviewing the draft report at that point, right? It's a short sitting day, so 4:30 to – whatever – 6.

Ms Pastoor: Mr. Chairman, I think that a lot of my caucus may be on their way to Lethbridge.

Ms Blakeman: Oh, right.

Mrs. Forsyth: All right. Just take October 28 off the calendar.

Ms Pastoor: We could fly out Friday morning.

The Chair: Okay. We can talk about October 28, 4:30 until whatever time, or – I keep getting these helpful hints over here – supper meetings the night of the 24th, the 25th, and the 26th, which is back to the earlier part of the week when we're coming into session.

Ms Blakeman: Well, as long as it's after session. I can do the night stuff, I think.

Mrs. Forsyth: I could do the 25th and 26th after session.

The Chair: The 25th and 26th. From what time?

Ms Blakeman: Well, 6:30.

The Chair: Can anyone tell me if that doesn't work them?

Ms Notley: Did you say the 25th and the 26th?

The Chair: Either day.

Okay. We've got some common ground. The 25th or the 26th at 6:30. Somebody please throw out a date, and we'll readily agree to it.

Mr. Quest: The 25th.

The Chair: The 25th.

Mrs. Forsyth: Mr. Chair, October 25 or 26 works for me.

The Chair: Wonderful.

Mrs. Forsyth: In the evening.

The Chair: And the 25th is a Monday?

Mrs. Forsyth: Correct.

Ms Blakeman: The first day of session.

The Chair: The first day of session, I hear.

Mr. Quest: So 6:30 until . . .

The Chair: Well, 6:30 until – give us a time, or do you need a final time?

Ms Blakeman: Well, let's say 8:30 at the latest.

The Chair: Okay. October 25 from 6:30 to 8:30 it is.

Ms Blakeman: Which is to review the draft report?

The Chair: Correct.

Mrs. Sawchuk, have we covered off all the dates that are required?

Mrs. Sawchuk: Mr. Chair, we still need one final date for the committee to adopt the final report on the record once we've completed the review of the draft. If there are any changes, staff are sent off to get all of that together. So it'd be a short meeting, knock on wood. I would assume an hour, maybe, some time in the first two weeks of November, and that's in accordance with the timeline that was originally adopted in April. November 15 is our final date.

Ms Blakeman: How much time do staff usually need to do the turnaround between a draft and a final, just on average?

Dr. Massolin: Well, Mr. Chair, it would depend on, of course, the substance of the report, but I think a week would be adequate.

The Chair: So you're suggesting the first week in November, Dr. Massolin?

Dr. Massolin: I think that would work. Yes.

The Chair: Okay. We've got that narrowed down. Can everyone look at their calendars at the first week in November?

Ms Blakeman: Could I suggest something? What about November 4 – that's an early session adjournment – at 4:30 or 4:45? Then people that are trying to get out of town can still get out of town.

The Chair: Okay. Does that work for everyone? A show of hands, quickly. November 4, 4:45.

9:30

Mrs. Forsyth: November 4, 4:30: I won't be able to make that, but don't go by me because this has been so challenging. That's a Thursday, and we need to get back into our constituency offices.

Mr. Groeneveld: If this is a short meeting, why are we doing it on the Thursday? Could we not on the 1st, 2nd, or 3rd, somewhere in there?

Ms Blakeman: Sure, but you guys usually end up with other meetings that push it off.

Mrs. Forsyth: I can do 1, 2, or 3, Barry.

Ms Blakeman: Okay. Yeah. I'm good for any of those.

Dr. Sherman: It's not likely I should be out of town the first week of November.

The Chair: Okay. I guess, to be very blunt, that if one person is going to be out of town, I'm not going to hold the meetings up for that.

Dr. Sherman: I'll get a sub.

The Chair: You'll get a substitute. Thank you very much.

Okay. I am going to take your advice, Mr. Groeneveld. Would the 2nd, a supper meeting, work? Yes? Ms Blakeman? Ms Notley?

Ms Blakeman: Starting at 6 something.

The Chair: At 6:17.

Ms Blakeman: Okay.

The Chair: This has been very challenging, and Karen Sawchuk has offered to read a motion that will cover all the dates for us.

Mrs. Forsyth: Barry, is the last date the 4th or the 2nd?

The Chair: It is the 2nd.

Mrs. Forsyth: Okay. Thank you.

The Chair: Ms Pastoor.

Ms Pastoor: Yes. I'm not sure that that's perfectly good for me or my caucus colleague. I think we have caucus dinner meetings on Tuesdays.

Ms Blakeman: Well, it's one happy meeting or another happy meeting.

Ms Pastoor: Yeah. Well, if the 2nd is good for everybody, then maybe we can wiggle ours around a little bit.

The Chair: Mrs. Sawchuk, will you please read a motion? We're going to take a vote.

Mrs. Sawchuk: Mr. Chair, I'm going to read what I think the committee has made their decision on: that the Standing Committee on Health revise the timeline adopted at its April 28, 2010, meeting by cancelling the September 13 and 14, 2010, meeting dates; adding meetings on September 27 and 29; that the October 28 meeting date be changed to the evening of October 25; and a final meeting be scheduled for November 2.

The Chair: You've heard the motion.

Mr. Groeneveld: Can we put the proviso: the 29th if needed?

The Chair: Yes, you can. As required. That'd be a friendly amendment, please, Mr. Groeneveld.

Mr. Groeneveld: Yes.

Ms Pastoor: Mr. Chair, could we have the times, please?

Mrs. Sawchuk: Did you want those in the actual motion, Mr. Chair?

Ms Pastoor: Well, then it's on the record, and we can check it when we find other ones.

Mrs. Sawchuk: Mr. Chair, a member will have to move this motion.

The Chair: Yes.

Mrs. Sawchuk: We'll do it one more time, that

> the Standing Committee on Health revise the timeline adopted at its April 28, 2010, meeting by cancelling the September 13 and 14, 2010, meeting dates; adding meetings on September 27 and 29 from 9:30 a.m. to 4 p.m.; changing the October 28 meeting date to the

evening of October 25 from 6:30 p.m. to 8:30 p.m.; and a final meeting be scheduled for November 2 from 6:30 p.m. to 8 p.m.

The Chair: Mr. Groeneveld has an amendment. The motion is made by Mr. Olson.

All right. Now Mr. Groeneveld is going to move that. Go ahead.

Mr. Groeneveld: The 29th that "if needed" be added. Very simple.

Mrs. Sawchuk: If needed, yes.

The Chair: All in favour? Opposed? That's carried.

Now, the amended motion, that Mr. Olson has moved, outlining all the dates. All in favour? It is carried. Thank you very much.

We have about six minutes before our first oral presentation. Dr. Massolin, can you give us a quick rundown of the overview of the documents posted on the website, please?

Dr. Massolin: Well, Mr. Chair, I think I can maybe handle the first one, but I don't think we would have time in the six minutes allotted to do all of them. I would perhaps make the humble suggestion that we look at a different time to do that if the committee wants to go over those documents and ask questions.

The Chair: Certainly. Are you comfortable if we do this under other business?

Dr. Massolin: Yes. Certainly.

The Chair: Later on we can do it all, then.

Dr. Massolin: Absolutely.

The Chair: Terrific. That gives us a little breathing time as we prepare for our first oral presentation, the Edmonton Police Service.

Is everything still quite clear, Heather?

Mrs. Forsyth: Mr. Chair, you keep fading out. Otherwise, if people just get closer to the microphone, that'll be fine.

The Chair: Okay.

Mr. Groeneveld: Mr. Chairman, what's the process? How are we going to conduct this?

The Chair: Okay. What we're going to do on each and every one of the oral presentations is that for the record we'll have them introduce themselves. We're going to introduce ourselves. There's a set time. They have 15 minutes to make their presentation, and that leaves us time to ask them questions. Unfortunately, we're going to have to stick to the times in order to make all of it work, so there's half an hour broken down in 15 and 15.

Mr. Groeneveld: Will there be a hard copy at the end of the day, or will it just be in *Hansard*? Is that how it's going to work?

The Chair: Mrs. Sawchuk.

Mrs. Sawchuk: Thank you, Mr. Chair. Yes, it'll be the *Hansard* record unless presenters hand in additional materials. We've also referenced their written submissions that were made, so those were available for the committee as well.

Mr. Groeneveld: Okay.

The Chair: All right. Well, moving on, I want to first thank Ms Karen Andersen, FOIP co-ordinator with the Edmonton Police Service, for coming in to make a presentation. Karen, before we start the presentation, I'm going to ask that everyone go around the table and introduce ourselves. And would our guest please give her full name and title for the record?

Ms Andersen: It's Karen Andersen. I'm the FOIP co-ordinator and legal counsel for the Edmonton Police Service.

The Chair: Thank you.

Ms Blakeman: Welcome, Ms Andersen. My name is Laurie Blakeman, and I'd like to welcome you to my fabulous constituency of Edmonton-Centre.

Ms Notley: Hi there. I'm Rachel Notley, MLA for Edmonton-Strathcona.

Mr. Vandermeer: Good morning. I'm Tony Vandermeer, MLA for Edmonton-Beverly-Clareview.

Mr. Lindsay: Good morning. Fred Lindsay, MLA for Stony Plain.

Mr. Elniski: Good morning. Doug Elniski, MLA for Edmonton-Calder.

The Chair: Our deputy chair is Ms Bridget Pastoor from Lethbridge-East, and I'm Barry McFarland, Little Bow, chair of the committee.

Mrs. Sawchuk: Karen Sawchuk, committee clerk.

Mr. Quest: Dave Quest, Strathcona.

Mr. Olson: Good morning. Verlyn Olson, Wetaskiwin-Camrose.

Dr. Sherman: Good morning. Raj Sherman, Edmonton-Meadowlark.

Dr. Massolin: Hi, Karen. Philip Massolin, committee research co-ordinator and table officer, Legislative Assembly Office.

Ms LeBlanc: Stephanie LeBlanc, legal research officer with the Legislative Assembly Office.

Ms Lynas: Hilary Lynas, director of access and privacy with Service Alberta.

Ms Mun: Marylin Mun, assistant commissioner with the office of the Information and Privacy Commissioner.

The Chair: All right. Well, thanks again.

Mrs. Forsyth: I'm Heather Forsyth, MLA for Calgary-Fish Creek.

The Chair: Sorry, Heather.

Thank you, Ms Andersen. You have 15 minutes, and then we'll open the floor to questions after you've made your presentation. Please proceed.

Edmonton Police Service

Ms Andersen: Thank you. I'd like to thank all of you for the opportunity to speak to you regarding the Edmonton Police Service's submissions for amendments to the FOIP Act.

As I believe you're aware, we have a significant number of access requests pursuant to the FOIP Act for all law enforcement agencies. For example, within the last annual reporting period the Edmonton Police Service alone had 268 FOIP requests. So we're very familiar with working with the act, the inquiry process, and the OIPC. In addition to our large number of requests, law enforcement information is unique. We've got special considerations, including the protection of our officers and the community. So I hope that I can bring you a different and an informative perspective from the Edmonton Police Service this morning.

9:40

In our written submissions we raised a number of points. I've tried to categorize them. I'll start with the two recommendations we made regarding disclosure of personal information. It would be our submission that the act needs to clearly allow for the disclosure of information to organizations and agencies that we work with in promoting programs and initiatives that are aimed at crime prevention and supporting participants in the criminal justice system. Currently if an organization is not a public body, the act can often hamper or even prevent us from sharing information that these community groups can use to fulfill their programs, to deliver services that individuals need.

We've also suggested that the act clearly allow for the sharing of information about perpetrators with victims of crime when it's appropriate. The Victims of Crime Act does allow for limited disclosure, but neither the Victims of Crime Act nor the FOIP Act allow for release of information with respect to an accused. For example, you have a domestic violence situation. It may be appropriate and in the victim's best interest to know the release dates, the conditions of release for an accused, and we're often not able to provide that information to them.

Regarding the application of the act section 4 identifies records that are not subject to the FOIP Act. By virtue of section 4(1)(k) records relating to ongoing prosecutions are not subject to the act. It would be our submission that records relating to ongoing investigations also have that same status and be excluded. There really isn't a rational basis for the distinction between the two. They're the same records, that are subject to the act until a charge is laid. The interest, I would submit, to be protected during an ongoing investigation is that the harm that could be done from releasing information from the investigation can be significantly higher than the harm at the prosecution stage. It would be our submission that the records would only be subject to the act at the completion of an investigation and/or prosecution.

There's an ongoing issue with respect to production of the same records to the same individuals. As an example, an individual who is unhappy with how he was treated when he was arrested may make a complaint to our professional standards branch, commonly referred to as internal affairs, under the Police Act. The professional standards branch will conduct an investigation, and that file may be hundreds of records. The individual goes to trial on his charges. That file is produced to the Crown as part of Crown disclosure, and the individual receives a complete or almost complete copy of the file through that criminal process. If the individual is unhappy with the chief's disposition of the complaint under the Police Act, he or she will file an appeal to the Law Enforcement Review Board. As part of the appeal process they will receive another copy of the exact same file.

Often the person is unhappy with other matters and will file a civil lawsuit relating to the event, alleging injuries during the arrest. As part of the civil process they will again receive another copy of the exact same file. They now have three copies of the file. Very little information is redacted because it isn't required during those court processes. The individual will then make a request under the FOIP Act. It's the fourth request for the exact same records. The FOIP process is actually the most time consuming as it requires more redactions of information, et cetera. It really becomes a duplication of time, energy, and resources, and it's an issue that really needs to be addressed.

I have noted that in a number of submissions other public bodies have made suggestions about a stay mechanism. We have suggested that if we know the applicant has the exact same records that it not be subject to the act. There are different ways of dealing with it, but it certainly needs to be addressed.

With respect to access to records section 10 of the act requires a public body to create a record that is in electronic form, using its normal computer hardware and software and technical expertise, and to create a record that would not unreasonably interfere with the operations of the public body. In our opinion, the exception created by this section has been interpreted very narrowly by the commissioner, particularly with the public body's obligation to re-create backup tapes that exist for disaster recovery purposes.

The cost, the time, and the effect on operations to re-create and search backup tapes is, in our submission, prohibitive. We would submit that the act needs to be clear that where the public body has to incur additional cost to fulfill an access request, including the backup tapes, this is an unreasonable interference with operations.

Section 20 of the act provides the discretion to not release information relating to law enforcement. Section 20(1)(c) allows us to refuse to disclose information that could reasonably be expected to harm the effectiveness of investigative techniques and procedures. In order for us to withhold information under this section, we have to prove a three-part test that goes to showing the harm. It's applied on a record-by-record basis and is often onerous and resource laden. One way of looking at it is to say that we have to spend considerable time and expense proving that telling bad guys how we're going to catch them is a bad thing. Often because of the three-part test, the type of information, we believe there is a harm, but we can't meet the test. Information can be detrimental, but sometimes people have a way of getting bits and pieces that on one view of it might not seem to be harmful, but if you get three different pieces and put them together, it might be.

In other jurisdictions there isn't that harm test. In Ontario it simply requires that there be a law enforcement investigative technique, and the law enforcement agency would have the discretion to withhold the information. It is discretionary, but it would give law enforcement the ability to not disclose information that we think is going to be harmful.

We would also suggest – and it's also in the Ontario legislation – a very clear exception that information can be withheld if it might endanger the life or physical safety of a law enforcement officer or any other person. It currently isn't in the legislation. It's arguable that it's within other subsections of section 20. It would be our submission that protection of our police officers should be clear and unambiguous. There should never be a question, and public resources shouldn't have to be used to argue about it. Currently we have to spend time and resources arguing about things where we're saying that officer safety is an issue.

Section 21(1)(b) relates to records exchanged between public bodies. The section currently requires that information be supplied in confidence in order for us to rely on that section. We're suggest-

ing an amendment that creates a presumption that records exchanged between police services and/or commissions are done in confidence.

Due to our significant number of requests we also probably have a significant number of matters in inquiry or review before the commissioner, and we've made a number of submissions about how we think that process could be a little more efficient and effective. We're asking that the commissioner be given more resolution options: to encourage informal resolution, to refer to mediation but only with consent of all the parties. They could conduct investigations but also have the ability to dismiss if appeals are frivolous, vexatious, or made in bad faith and the ability to refuse to conduct an investigation or an inquiry.

9:50

We're submitting that the mediation and investigation processes conducted by the OIPC be clearly separate and distinct in the act and that the same person not be the mediator and investigator for the same matter, which currently could happen. Information can't necessarily be disclosed freely in mediation if the exact same person is then going to be appointed to investigate and write a report and findings about it.

We're also asking that investigative reports that are done by the OIPC be put before the adjudicator. The time, expense, the knowledge that's obtained during the investigative process shouldn't be excluded. It should be used and make the inquiry process more efficient. We would, however, suggest that the investigative reports not be made public without the consent of the parties. The investigative process doesn't import the principles of natural justice and fairness, so allegation statements can be made that are not challenged by the other party. Findings can be made that aren't subject to cross-examination. To have those findings made public without those rights of challenge, we'd submit, is not appropriate without the consent.

Section 71 of the act sets out the burden of proof at inquiry. It's our submission that the section should be amended such that the public body needs only to establish that it applied the exceptions in a reasonable manner. There should be some recognition that the public body is the expert at administering the act with respect to its own particular records. The administration of the act requires judgment calls, weighing and balancing of different considerations. Two people can look at the same matter and have two different opinions, and both can be correct under the act.

It's our submission that the judgment of the people that deal with the same records, that are the experts in their area, for example law enforcement, should be deferred to if it's reasonable. The standard review should not be for an adjudicator to substitute their own opinion when there was a reasonable one that was made in the first instance. As an example, if we have an officer in charge of a training section that states that information could reasonably jeopardize the safety of police officers and that opinion is reasonable, it should be respected. They're in the best position of anyone in the inquiry process to make that call.

I know that there have been a number of submissions about the issue of privilege and the effect of the Supreme Court of Canada decision, the Blood Tribe decision as it's often referred to. I would just like to add or point out that solicitor-client privilege is fundamental to the proper functioning of our legal system. It has to be as close to absolute as possible, and it has to be that way to ensure public confidence and retain relevance. It would be our submission that in order to maintain those principles as confirmed by the Supreme Court, it should be set out that only a court has the ability to compel and review privileged documents.

We made some submissions about being named affected third parties, and it would be our submission that if records created by a police service are at issue in an inquiry, then the police service should be automatically named as an affected third party and given an opportunity to make submissions about our records. For example, if we have given records to the Edmonton Police Commission in confidence, if they receive a FOIP request and the matter goes to inquiry, we would like to be named as affected third parties and given the opportunity to speak about the disclosure of our own records.

The orders affecting our records could have significant impact on our organization, the individuals that are named in there, and how we process our own requests. We obviously have no control over the submissions of other public bodies, but we're in the best position to make arguments about them. In the past we've been required to make written submissions to the OIPC adjudicator as to whether the chief is a person and whether they should be named as an affected party when it was the chief's records at issue. I would submit that that's not an appropriate use of public resources, and there should be an automatic right to participate.

Those are the submissions that I have prepared.

The Chair: Thank you very much, Ms Andersen. I'll open it up to questions that we might have for you now.

I do have at this point Mr. Elniski.

Mr. Elniski: Thank you, Mr. Chairman. Just to go back to earlier in your conversation, you talked about records and sealing the records at the completion of an investigation or a prosecution. You had made a comment, and I just want to clarify this. What happens if there is an investigation and then subsequently no prosecution?

Ms Andersen: Currently?

Mr. Elniski: Well, currently. What's your proposal under the legislation?

Ms Andersen: It would have to be clarified. There would have to be a distinction between an ongoing investigation and an investigation that we considered concluded. If it was concluded, then I would say that they would be subject to the FOIP Act. For whatever reason if it's concluded – it could be a number of reasons – there wouldn't be the harm to an ongoing investigation from, you know, disclosing something to a suspect. Obviously, at that point there wouldn't be a suspect, or it wouldn't be concluded, for example.

Mr. Elniski: Okay. Good. Thank you.

Just a supplementary question, Mr. Chair. You talked very early on about organizations that are not public bodies that you deal with. Can you give me an example, please, of one or two of those?

Ms Andersen: Boys and Girls Clubs, the community solution to gang violence, Native Counselling Services.

Mr. Elniski: Okay. Perfect. That's exactly what I thought. Thank you very much.

The Chair: Thank you.

Next question. Laurie Blakeman, followed by Rachel Notley, please.

Mrs. Forsyth: Chair, can you add me, please?

The Chair: You bet.

Mrs. Forsyth: Thank you.

Ms Blakeman: Thank you very much. I'll start with a couple of questions, and if you can put me back on the list, please, Mr. Chair.

I, too, was struck by the very high number of requests that the police service has had to process, but one of the things that occurred to me was the particular year that we were looking at. Are you able to tell me whether that trend has continued or whether we had the high number of requests because of that exceptional year which included the unauthorized searches of the CPIC around what's commonly referred to now as – the one with the reporter and the chief of the Police Commission. It was discovered there were unauthorized searches of the database, and that engendered a whole bunch of other people searching to see if their personal information had been accessed. Are we referring to the same year, and are you able to tell me if in subsequent years the number of requests has been as high?

Ms Andersen: Our requests have been fairly constant at about 300 or slightly under. This year, to extrapolate, we're slightly under, but I don't think that that matter had a significant spike in requests. We still have a number of requests from people asking: who ran my name?

Ms Blakeman: Oh, yeah. It did spike. From the previous year to the year this happened, it quadrupled.

Okay. My second question is that the police service has appeared before this FOIP review committee previously and had raised a number of requests which were rejected on the grounds that the committee didn't want to put them in place. Of the requests that you've made this time, how many are new, or how many of them are you repeating from your previous ones?

Ms Andersen: I couldn't answer that. I wasn't a member of the service or part of the previous submissions.

Ms Blakeman: Do you have access to that previous submission to the committee? Maybe you could provide the information after the fact in writing.

Ms Andersen: I could certainly try.

Ms Blakeman: Okay. The final question in this set. The question around wanting to provide information to third parties who on the face of it appear and are, in fact, well-loved and very necessary organizations like Boys and Girls: I'm seeing a trend to move towards more policing done by volunteers in the community, less by the professional police officers. I can see a point in the future where we lose control of that information if we have beat cops, for example, that are a completely volunteer organization. How far does the police service expect this to go? Do they see a limit on the amount of information that they would be providing to these organizations? How do you ensure the privacy given that these organizations are not subject to the same act?

Ms Andersen: Well, I think that no one is suggesting that there would just be unlimited information that would be provided. It would have to be identified as to what was necessary for their needs to deliver their programs. Only things that were essential would be given to them.

10:00

I cannot speak to the requirements of PIPA, but organizations normally have their own obligations on what they can do. We do a lot of memorandums of understanding as to what happens with information to ensure that organizations we're sharing with treat information appropriately, have appropriate security, destruction, retention. It's returned to us if appropriate. So we take great safeguards now with the information that we're able to share, and we would certainly continue to do that.

Ms Blakeman: Have you done a risk assessment of what would be likely to happen to information that was passed on to groups operating in the community?

Ms Andersen: Not in this context, no.

Ms Blakeman: Okay. Thanks.

The Chair: Thank you.

Ms Notley, followed by Mr. Lindsay.

Ms Notley: Thank you. I just have two quick questions, and I'm sorry if one of them you actually gave us the answer to and I missed it. We talked about the number of requests that you get on average each year. Then you had also talked about people making repeat requests. What's your average number of requesters per year?

Ms Andersen: I don't know. In the example I gave regarding individuals with the same legal matters – the Law Enforcement Review Board, civil litigation, et cetera – they're often represented by the same counsel. So we have a lot of the same law firms that we deal with, for example, but they're acting on behalf of different individuals.

Ms Notley: Right. I guess what I'm trying to get at is the complaint that you raised that, you know, there are people that are making request after request after request. I just want to know how big a problem it is.

Ms Andersen: In the example I gave, there is one FOIP request, but we know they have the exact same records because we've given them to them in different processes. They're certainly entitled to their information in the appeal, in the litigation. We're not suggesting they're not entitled to them. But at the point in time when we know they have the same thing three times and they make a FOIP request, how is that fulfilling the . . .

Ms Notley: What you're suggesting, then, is that it's not that they're making requests over and over; it's just that they're making a FOIP request.

Ms Andersen: For information that we know they have, that is identical.

Ms Notley: Right. But they don't necessarily know that you've given them all the information. It's been given to them under different criteria and different rules, so they don't necessarily have a way of knowing that they've gotten everything that you have.

Ms Andersen: If we've said three times, "This is the entire file," would we change our mind the fourth time?

Ms Notley: I don't know. I guess it depends on how information is created from day to day. I mean, I've done enough of this to know that you get the entire file, and then you discover another document or another document is created or whatever.

I'm sorry; that's fine. I appreciate the clarification, though, because I had understood you to be saying that there were people making similar FOIP requests over and over and over again.

Ms Andersen: Well, we occasionally do, but I wouldn't consider that to be a significant problem.

Ms Notley: Right. Okay.

Now, I want to go back to a line of questioning that Mr. Elniski had raised. I just want to get some clarification on this, which is this whole issue of excluding information from application of the legislation where there's an investigation that is ongoing. It's been my experience in the past that the sort of parameters around that status are a little fuzzy. So we are in a situation where something is, quote, under investigation, but it can be under investigation from time immemorial. Everything attached to it then becomes hidden from public view.

Does the Edmonton Police Service – and I'm not saying that it's just with respect to the Edmonton Police Service. I think there's a variety of contexts within which things are under investigation. It's not just, certainly, in your scenario. Do you have concrete parameters, rules, criteria around when a file is open and when a file is closed to give us some guidance? Otherwise, it seems to me that there's a great big exemption and a door that's opening that nobody can touch or feel the lock or the latch to.

Ms Andersen: To give you an exact answer to that, I would have to get back to you as to the current policy with our new EPROS system and our new gateway as to how the system and the boxes are checked to show. I could certainly do that.

Ms Notley: Okay. That would be helpful.

Thank you.

The Chair: Thank you, Ms Notley.

Mr. Lindsay, followed by Mrs. Forsyth.

Mr. Lindsay: Thank you, Chair. I just wanted to question when you spoke about disclosure concerns regarding investigative processes and techniques. I know that's a concern for all policing agencies. My understanding was that that came up during a discovery process through the court process. How does FOIP get involved in that, or is FOIP what gives the courts the right to disclose those techniques? Could you comment on that?

Ms Andersen: Sorry. I'm not quite understanding the question.

Mr. Lindsay: You spoke about the concern that police agencies have in regard to disclosing information as to how they've arrived at laying charges involving an investigation, and, you know, you brought that up as a FOIP concern. My understanding is that that concern was more around disclosure when the matter went before the courts. I just wondered if it's a disclosure process in the courts because of the FOIP legislation or whether there's something else that's in addition to what takes place in the court process.

Ms Andersen: I would think that the criminal justice process certainly is separate and has separate rules, and it would be a matter of relevance. If it was, you know, a very serious matter, there could be closed courtrooms, that type of thing, to deal with it. That would be part of the criminal justice system, which is completely separate from the types of information that we're talking about.

This would be more: tell us how you train the canines and how you're going to use them to catch me. The position of the Edmonton Police Service might be: we don't want to release that because that's going to potentially tell you how to get away; it's going to potentially harm a police officer or harm the dog. We've had issues as to, you know, whether that's appropriate or not. We've had inquiries about that type of information.

This is more general. It's separate from what comes out in the criminal process if that answers your question.

Mr. Lindsay: Yeah. Thanks for that. I didn't realize that there actually had been FOIP requests of that type of information. I knew it came up in disclosure. Anyway, thank you very much for that.

The Chair: Thank you, Mr. Lindsay.

Unfortunately – and I'm sorry, Mrs. Forsyth – we've reached our time allocation on this oral presentation. We want to thank you, Ms Andersen, for making your presentation.

Mrs. Forsyth: Mr. Chair, if I may.

The Chair: Yes.

Mrs. Forsyth: This is to the committee. Because of the short timeline could we possibly keep one question to every member at this particular time instead of a supplement question? They can go back on the list. At least that gives opportunity to some of us that would like to have a question.

The Chair: Good suggestion, Mrs. Forsyth. In fact, I was going to make that before the next one came up. In fairness, we had four more individuals. If you want, if it would help, I don't mind taking the questions they had, and perhaps we can follow up with this presenter so that each of you that didn't get to ask a question could perhaps get an answer from Ms Andersen at a later time but before the draft is done.

Thanks again for your time, Ms Andersen.

Ms Andersen: Thank you.

The Chair: While we're having the next group come up, Heather, would it be possible that you and anyone else that had another question could quickly put it on the record, and then the transcript or some mode of communication could be sent to Ms Andersen?

Mrs. Forsyth: Yes. I just closed my book, so if you can maybe get one of the other members first and then come back to me.

The Chair: Verlyn, did you have your question ready?

Mr. Olson: Well, my question was just going to be regarding the reference to section 20 and the ability of the public body to refuse to disclose information on the basis of it being harmful to law enforcement. I think Ms Andersen said that that section is probably worded broadly enough to include officer safety, but it does not specifically mention officer safety. So I was just going to ask if this has been the subject of any appeal or any process or whether it's just something that has been identified as a potential issue without having actually been an issue. Okay. That was just my question.

10:10

The Chair: Okay.

Heather.

Mrs. Forsyth: Thanks, Barry. What I wanted to ask the Edmonton Police Service: when I was chairing the safe communities task force, we repeatedly and consistently heard from Albertans and all police forces across the province about the serious concerns they had about the current legislation acting as a barrier on sharing information amongst police services, the community agencies, schools, health regions, et cetera. I just wanted to get a clarification from them if it's working – and I'm still hearing that it isn't – and what recommendations they would have to get rid of that barrier.

The Chair: Thank you, Heather.

Mrs. Forsyth: Thanks.

Mr. Groeneveld: Very quickly, Chair, I just wanted to know if this was strictly the Edmonton Police Service or whether they had collaborated with any of the other police services to put this together for us.

The Chair: Very good. Thank you.

I apologize for that, but we're going to try to correct it by limiting one question per member. Then, if there's time, we'll come back to the others.

Ms Blakeman: Sorry. I did have additional questions. The exceptions to disclosure with one police service to another, my understanding is that those records are only disclosed now with consent. Your recommendation would make every communication between police services subject to consent. Can I get an example of where something that you've been required to disclose has been provided by another police service? So there's that question.

Also, further to Ms Notley's question about the ongoing investigations, had the Edmonton Police Service considered a time limit, some sort of time parameter around that?

Thank you.

The Chair: Thank you very much.

Moving right ahead, our next presenters are the Alberta Weekly Newspapers Association. Before we start the presentation, I'd ask that we go around and introduce ourselves. I'll ask first if our guests would give us their full names and their titles for the record for *Hansard*. Please proceed.

Mr. Merrell: I'll start. I'm Dennis Merrell. I'm executive director of the Alberta Weekly Newspapers Association.

Mr. Bachynski: I'm Brian Bachynski. I'm a board member for AWNA.

Ms Blakeman: Laurie Blakeman. I'd like to welcome you to my fabulous constituency of Edmonton-Centre.

Ms Notley: Rachel Notley, MLA, Edmonton-Strathcona.

Mr. Vandermeer: Good morning. I'm Tony Vandermeer from Edmonton-Beverly-Clareview.

Mr. Groeneveld: George Groeneveld from Highwood.

Mr. Lindsay: Good morning. Fred Lindsay, Stony Plain.

Mr. Elniski: Doug Elniski, Edmonton-Calder.

Ms Pastoor: Bridget Pastoor, Lethbridge-East and deputy chair.

The Chair: Barry McFarland, Little Bow, chair.

Mrs. Sawchuk: Karen Sawchuk, committee clerk.

Mr. Quest: Dave Quest, Strathcona.

Mr. Olson: Good morning. Verlyn Olson, Wetaskiwin-Camrose.

Dr. Sherman: Good morning. Raj Sherman, Edmonton-Meadowlark.

Dr. Massolin: Good morning. Philip Massolin, committee research co-ordinator and table officer, Legislative Assembly Office.

Ms LeBlanc: Stephanie LeBlanc, legal research officer with the Legislative Assembly Office.

Ms Lynas: Hilary Lynas, director of access and privacy with Service Alberta.

Ms Mun: Marylin Mun, assistant commissioner with the office of the Information and Privacy Commissioner.

The Chair: And one in the air.

Mrs. Forsyth: Hi, Dennis. I'm Heather Forsyth, Calgary-Fish Creek.

The Chair: Very good.

Thanks, gentlemen. You have 15 minutes for your presentation, and then I'll open the floor for questions, which you came into at the last. Hopefully, we're going to make it a little quicker and cleaner for you. Please go ahead and do your presentation, and then we'll ask some questions.

Alberta Weekly Newspapers Association

Mr. Merrell: Well, thank you, Mr. McFarland and committee members. Thank you for the opportunity to present today. I bring regrets from our president, George Brown. He had intended to be here but was called away on some business.

I'll just give a bit of a preamble. We represent 118 community newspapers from around the province. Because our membership is many and varied, we decided to conduct a survey and just really get a sense of what experience our members were having with FOIP requests and with the legislation in general. We did receive 42 responses, which we felt was a pretty good cross-section. It gave us a good indication of the experience that's out there.

There are a few observations and some concerns, I guess. One of them is the fact that two-thirds of those who responded said that they hadn't really actually carried out a FOIP request. We'll get into that a little bit later. But the kinds of things, I guess, or the types of information that our members would request would involve municipal budgets, quite frequently they want access to schools to take photographs of students during their activities, coverage of the courts, that type of thing. Those are the types of stories and photos that the community newspapers would be running into FOIP on.

I guess there are three primary concerns with respect to those that have made requests. The lengthy time it takes to have those requests processed would be one. Cost was another factor that was given. Community newspapers tend to have pretty limited budgets, so cost

was definitely a concern. Also, thirdly, I think a general feeling that there was a lack of maybe good information out there in the people that they were dealing with in terms of their understanding of FOIP. An example might be a lot of newspapers really feeling they were stonewalled. When it came to coverage of schools, generally met with the response of: well, FOIP; we can't give you that information. But they don't really, truly understand why they're saying that. I mean, there's just not a good enough general, overall understanding when dealing with people who are charged with carrying out FOIP legislation. Do they really, truly understand the legislation? I think the thinking out there among our membership is that perhaps not.

At that point, I think I'm going to turn it over to my colleague Brian for a few more specific kinds of concerns.

Mr. Bachynski: Thanks, Dennis. I'll just elaborate on a couple of the points that Dennis raised. I'll start with the timelines. Of the two-thirds of AWNA members who obtained access to the information they requested, half of them were dissatisfied with how long it took for their request to be processed. That's a concern for journalists. One of the mandates of the media is to inform and, by doing so, help protect the public. A key method by which the press achieves this objective is by scrutinizing the activities of government bodies. Its ability to do so in an effective and timely fashion is crucial to a democratic society. The legislation currently provides a 30-day response period, which our members feel is much too long, and that can be extended in certain circumstances. The Alberta Weekly Newspapers Association recommends that in emergent situations, where the nature of information sought requires a quick response, a process be put in place whereby access requests may be processed on an emergency basis and the individual seeking access will receive a response within 48 hours.

The second point that was raised by our members is the access fees. They thought that the cost was quite prohibitive. Smaller rural newspapers do not have the operating budgets of larger daily newspapers. Nearly half of the AWNA members surveyed, 41.7 per cent, indicated that the cost associated with access requests posed a concern. The AWNA recommends that the regulation be amended to include an exception that waives access costs for journalists working for smaller newspapers. Alternatively, the AWNA recommends that a reasonable flat annual fee be charged which would cover all the newspaper's costs associated with FOIP.

10:20

Dennis also touched on a concern with actually dealing with the personnel. Over the course of making access requests, many AWNA members were left with the impression that the public body personnel processing their requests need a better understanding of the legislation and how it was intended to operate. In particular, the understanding of what information is subject to FOIP needs to be improved as this would reduce the number of unnecessary access requests and conserve the scarce resources of both public bodies and the organizations seeking information. Several of the survey respondents expressed reservations about the treatment they receive when making FOIP requests as they were made to feel like an unwelcome nuisance, like it was kind of a bother. This is a serious concern in light of the fact that there is a right to access this information.

The purposes of FOIP are contained in section 2. One of its purposes is "to allow any person a right of access to the records in the custody or under the control of a public body subject to limited and specific exceptions as set out in this Act." This section makes it clear that the right of access is subject to exceptions that are limited and specific in nature. However, the default position adopted by those administering access requests is one of nondisclosure, thereby creating the perception that public body personnel hide behind FOIP.

A better understanding of the legislation could address this. The AWNA is recommending that personnel who interface with the public and respond to FOIP requests be better schooled in the purposes and operation of FOIP, including that the right to access information is broad and subject to exceptions that are limited and specific in nature and the details of those exceptions.

It's also felt by our membership that there is a general perception out there that FOIP requests are complicated and quite onerous. Whether or not that's the reality is a different story, but that perception does exist out there. The AWNA is recommending that those who interface with the public and respond to FOIP requests be better schooled to assist in the wording of access requests so as to assist those making requests in wording requests so as to obtain what they are seeking.

Dennis, maybe I'll pass it over to you now to talk a little bit about why so many AWNA members avoid FOIP.

Mr. Merrell: Well, I mean, we pretty well pointed it out in our presentation. I think a lot of our members are feeling that, you know, they're getting stonewalled in a lot of cases. It's a costly process. It's just that for a lot of our members, I mean, going about their daily and weekly business of putting out a newspaper, it's more trouble than it's worth for a lot of them, unfortunately. In conclusion, it's mainly that there just needs to be, I think, more training or more information, maybe more even we use the word advertising of what FOIP is really all about.

I just think that would serve our members a little better, if they felt that there was a general, overall better understanding out there among people in public bodies that are serving us, that they have a better grasp of FOIP. I think that really, in a nutshell, is kind of the biggest point that we could bring to the table today: just improve the training and the information that's out there so that we're not running into situations where, in our case, stories and photos aren't getting into the newspapers not because they shouldn't be but because somebody doesn't understand that, well, really, that is within the guidelines, or allowable.

It's basically, as Brian said, that unfortunately the default position would often be, "Well, no, you can't have that information" because people are afraid, I think, that they'll make the wrong decision or make the wrong call. They just don't understand it well enough.

I think that would probably conclude what we have to present other than what's in our written report.

The Chair: Thank you very much. It might even give us a few more minutes for questions, then. We appreciate it.

I'll go through the list in case I've missed anyone: Ms Blakeman, Mr. Olson, Mr. Quest, Ms Notley, and I might even have a question.

Ms Blakeman, please.

Ms Blakeman: Great. Thanks very much. I know that the city of Edmonton has moved to an open data system, and I'm wondering if you had any suggestions about categories of information that could routinely be disclosed on a website that would make your work less onerous in trying to get information from government. Are there specific areas that could, you feel, be routinely disclosed on a website or in an open-source data system?

Mr. Merrell: I'm not really sure I've got an answer for that one.

Do you have anything you want to add on that?

Mr. Bachynski: No, I don't.

The Chair: Perhaps you could think about it and get back to us.

Mr. Merrell: We will think about that, though. Yeah.

The Chair: Thank you.
Mr. Olson.

Mr. Olson: Thank you, and thank you for the information today. My question is regarding your suggestion that there be the ability to get information more quickly, within 48 hours, in an emergent situation. Can you talk a little bit about what you would see as an emergent situation, how that would be defined in any legislation, and who would make that call?

Mr. Bachynski: Sure. We're weekly newspapers, so, you know, we have a week to gather information, essentially. With the way FOIP requests work now – Dennis touched on it a little bit – quite often newspapers will try to access information about municipalities in which they are located: municipal budgets, expenses, documents, maybe some personnel issues surrounding those particular things. Those issues are in the communities, and they are important to the readership. If the journalists cannot do their job and report because they can't access the information that they're asking, that would be an emergent situation. If they try to access through FOIP and it takes 30 days, the story is then 30 days old, and the relevance to the community has probably passed. That's what an example of an emergent situation would be.

Mr. Olson: Well, it sounds to me like pretty much everything would be an emergent situation, right?

Mr. Bachynski: I wouldn't say that everything would be an emergent situation, but I think the feeling of the membership is that the 30-day window is far too long. We work in newsgathering. That's what we do. News needs to be reported in a timely fashion, and 30 days is a roadblock to getting that information to our readership.

Mr. Olson: Okay. Thank you.

The Chair: Thank you.
Ms Notley, please.

Ms Notley: Yes. I just wanted to get a little bit more information from you in terms of your thoughts around the fees. You mentioned the notion of a reasonable fee. First, obviously, you talked about an exception for journalists, and that's great. Personally, I'd like to see an exception for all members of the public. But if we don't go there, on the basis of your membership, for smaller newspapers who have tight budgets, what in your view would be a reasonable fee?

Mr. Merrell: We haven't really given any thought to what a fee would be. I know that in some jurisdictions there are, you know, reasonable, almost nominal fees. I think recouping costs, perhaps. Like, if there's a way to set fees so that it's – I mean, in our case I like the idea of an annual fee. What that annual fee could be: I would say in the range of a few hundred dollars, maybe, annually. Would it cover the kind of clerical costs associated with it? I'm not sure. I'm just not aware of what all the costs involved would be, I guess. That's part of it. But I just know what restraints there are on many of our newspaper budgets, the smaller papers, so it kind of struck us that an annual fee might be a way to go on that if there is a way to structure it with a view, like I say, to recouping the costs associated with the people that are processing those requests, I guess. We'd probably need a little bit more information around that before proposing what we would feel would be reasonable.

Ms Notley: Thank you.

The Chair: Ms Pastoor, please.

10:30

Ms Pastoor: Thank you. You spoke about your time frames, which I'm sure we can all appreciate are very important to be able to get the news and the information out to the general public. I wonder if you could comment on the helpfulness of the communications staff in public bodies. Presumably, they're the ones that are there to answer the questions, and there would be no cost. That's their job. What better services from communications do you think might be an alternative that would actually help our reporters get the information to the public?

Mr. Bachynski: I can speak to that a little bit. Maybe you can, too, Dennis. The feeling from our membership when they're requesting information is that they're almost intruding on the communications staff and that they're kind of being a bother. That could be easily solved by perhaps just more direct, more timely – more courtesy extended from the staff. The membership feels that, you know, when they're making the call, they're kind of being roadblocked and stonewalled and they're not really there to help.

Mr. Merrell: Well, I guess that just a customer service attitude and approach I think would be the word of the day there. I mean, it's just really obvious from our survey. We were getting some feedback that some people felt that they were getting that kind of attitude, that they were being accommodated as opposed to the public having a right to the information and that we're requesting it to convey it to the public. I think it's fair to say that it's your job to kind of provide that information. There's just generally a sense that that spirit of serving the public maybe wasn't quite there in terms of information requests.

Ms Pastoor: I think that in your original presentation you were speaking about that in terms of sort of the FOIP staff, and I think I'm speaking more in terms of the communications staff. You should be able to go to whatever ministry's communication and ask directly to them – that was my thrust in that question, not necessarily the FOIP staff – because that's their job, to get the information out to the public, and it is free.

Mr. Merrell: Yes, and that's a good suggestion because I think the actual rank and file at our newspapers probably really aren't too tied into those communications folks, and that's probably part of the trouble there. Perhaps there needs to be a little bit more work around that in terms of reaching out to those kind of folks rather than dealing with people that – well, you know, really, I guess what I'm trying to say is that I just don't think the average reporter or editor out there in, say, Provost, Alberta, would know that, okay, this is the person I need to talk to in this ministry who is the communications person. So that communication probably just isn't taking place, I would guess.

Ms Pastoor: I guess my question was whether you had received, you know, what you think to be adequate public service from the

communications, but I'm not sure I got an answer to that. Perhaps you can think about that as well for those that do use that route.

Mr. Merrell: Yeah.

The Chair: Thank you. My question to you was in relation – and I'm glad you brought up the school situation. We had experience in the past – I stress in the past – where a school may have been told that they had to take down their graduation class pictures for 50 years because it was contrary to FOIP. That kind of blew me away, got me pretty upset. On the other hand, we had another weekly paper that did an absolutely incredible job of covering young athletes in schools and school activities, which I think is very admirable. So I think I understand where you're coming from. Have you got some other examples of the kinds of things that are being detrimental to good reporting?

Mr. Merrell: Well, certainly, I mean, pretty much every newspaper does a grad issue, I would think – when FOIP came in, all of a sudden, you know, you can't go out and take photos – kind of reminding the schools that, well, it's actually a public event, and we should be able to take photos and that kind of thing. That's one example and, I guess, taking sports photos and that kind of thing. Again, at what point is it really coverage of a public event kind of thing that should be allowed to be photographed and appear in the newspaper, and at what point is it, well, we have to really protect the identity of these children under our care in the school? I just don't think there's enough understanding there, I would say, across the board on what the delineation is there.

The Chair: It may help us help you if you could identify the areas because maybe some of advanced – I'm sorry; I'm almost going into two questions here. If you could help us, then maybe we just need to smarten a couple of areas up instead of the whole thing.

Mr. Merrell: I think certainly that's a fair question. I mean, we could come back with some specific instances where members feel that very definitely they've been unfairly blocked. We can certainly do that.

The Chair: Thank you.

Dr. Sherman, and then if we have no others on the list, we'll have Ms Blakeman.

Dr. Sherman: Have you worked with the FOIP office and other public bodies just to streamline the process for you to gather information and prioritize what for you is an emergency or urgency and, at the same time, educate your membership – a lot of it appears to be that your members don't understand a lot of this – on what's appropriate, what's not, and where you can actually save expenses?

Mr. Merrell: We would certainly welcome working with you on your helping us to help our members in that regard for sure because there has probably not been enough information going out to our own members to really get them more familiar with it. The fact that so many of them aren't even bothering tells us that, definitely.

The Chair: Thank you, Dr. Sherman.

Back to Ms Blakeman, please.

Ms Blakeman: Thanks very much. On page 4 of your submission under section (d), complicated procedure, you're suggesting that it's difficult to word a request so that it adequately covers the subject that you want the information on and that you're getting back a response of "no records found" and that if you don't, then it's so broad you're paying a lot of money to get it. Now, the commissioner has said that a search must retrieve all records, quote, reasonably related to the subject of the request. Can you give this committee any example of a case where a public body had or should have had a record but responded that no records were found? I know that you think there's a perception that it's a problem; I'm just looking for specific examples of where it's a problem.

Mr. Merrell: We might have to delve a bit deeper into that because the results of the survey didn't really give us that kind of really specific information. It was kind of more general.

Mr. Bachynski: We can certainly follow up with the members that responded in that vein and get an answer for you.

Ms Blakeman: Okay. Thank you. Through the clerk, please.

I'm curious about your wanting what you call a reasonable fee or a possibility of an annual fee. I notice that 66 per cent of your members didn't even use FOIP. For whatever reason they perceive it's difficult, and you mentioned perhaps an annual fee of a couple of hundred dollars. So if the FOIP fee now is $25 and you're suggesting, let's say, $250, that's 10 FOIP requests per year. Is that what you had in mind when you were suggesting that? Would you consider as well any top limits so that you didn't have someone for a flat fee making a thousand FOIP requests a year? Can you flesh that out a little bit so that we can consider it more thoroughly?

Mr. Merrell: Well, I mean, the reality is probably that some of our members would even balk at paying anything, to be honest with you. Certainly, the ones that are active and would be making multiple requests – and a number of those surveyed are making those multiple requests – I think would probably feel that, you know, just paying one annual fee would definitely be preferable. But the 67 per cent that were dissuaded from using it maybe felt that just on general principle they didn't want to have to pay for this public information. So that would be again a tough one to really say. Is there a general rule of thumb that would apply to 118 different publishers? I don't think so.

10:40

Ms Blakeman: Okay. I'm trying to help you here. Work with me. If you're asking us to consider a special category to give weekly newspapers a flat fee, is there anything else you can add to that as we consider this? You know, is the $25 reasonable? Would you be looking at something like no more than 20 requests for $250? If I'm going to seriously take this forward to the committee, give me something to work with.

Mr. Merrell: I'll have to get back to you on that. I don't have an answer.

The Chair: Thank you very much, gentlemen. We look forward if you can supplement some of the questions later on. We really appreciate your coming in this morning. On behalf of the committee thank you very much.

Mr. Bachynski: Thanks for hearing us.

The Chair: To the committee members, we're now going to take a very short break, and in exactly 10 minutes we're going to hear from our third presenter.

[The committee adjourned from 10:41 a.m. to 10:51 a.m.]

The Chair: Welcome back, everyone. Prompt and courteous. Gentlemen, it's our third presentation, and before we start it formally, I'd ask that we go around the table and introduce ourselves as well as our guests. If they would give their full names and their titles for the record. We'd like to begin with you gentlemen, please.

Mr. Saher: Good morning. Merwan Saher, Auditor General. With me today is my legal counsel, Kerry Langford.

Mr. Button: Good morning. Gord Button, Alberta Ombudsman. With me this morning also is my senior legal counsel, Joanne Smart.

Mr. Wilkinson: Good morning. My name is Neil Wilkinson. I'm the Ethics Commissioner, and with me this morning is our corporate counsel, Brad Odsen.

Mr. Fjeldheim: Good morning. My name is Brian Fjeldheim. I'm the Chief Electoral Officer. No one is with me this morning.

The Chair: Very good.
And our eye in the sky?

Mrs. Forsyth: Hi. It's Heather Forsyth, the MLA for Calgary-Fish Creek.

The Chair: Thank you.

Ms Blakeman: My name is Laurie Blakeman, and I'd like to welcome each and every one of you to my fabulous constituency of Edmonton-Centre.

Ms Notley: My name is Rachel Notley. I'm the MLA for Edmonton-Strathcona.

Mr. Vandermeer: Good morning. Good to have you with us. I'm Tony Vandermeer, MLA for Edmonton-Beverly-Clareview.

Mr. Groeneveld: George Groeneveld, Highwood.

Mr. Lindsay: Good morning. Fred Lindsay, Stony Plain.

Mr. Elniski: Good morning. Doug Elniski, Edmonton-Calder.

Ms Pastoor: Good morning. Bridget Pastoor, MLA, Lethbridge-East and deputy chair. I also, like Brian, sort of feel naked without my legal counsel.

The Chair: I'm going to welcome you at some point to Little Bow if you're ever down there. My name is Barry McFarland, and I'm chairing the committee.

Mrs. Sawchuk: Karen Sawchuk, committee clerk.

Mr. Olson: Good morning. Verlyn Olson, Wetaskiwin-Camrose.

Dr. Sherman: Good morning. Raj Sherman, Edmonton-Meadowlark. I've got my legal counsel right beside me.

Dr. Massolin: Good morning. Philip Massolin, committee research co-ordinator and table officer, Legislative Assembly Office.

Ms LeBlanc: Stephanie LeBlanc, legal research officer with the Legislative Assembly Office.

Ms Lynas: Hilary Lynas, director of access and privacy with Service Alberta.

Ms Mun: Marylin Mun, assistant commissioner with the office of the Information and Privacy Commissioner.

The Chair: Well, thanks for all the introductions and the good-natured comments.

You now have 15 minutes to make your presentation. I don't know how the four of you have split it up, but at the end of the day we'll cut you off, then we'll ask you some questions, and at the end of the time here we'll complete our presentation with you. Please proceed.

Officers of the Legislative Assembly

Mr. Button: Thank you. As I already stated, my name is Gord Button, and I'm the Alberta Ombudsman. On behalf of my fellow Leg. officers here this morning – the Auditor General, the Ethics Commissioner, and the Chief Electoral Officer – I'd like to thank the committee for the opportunity to speak to our joint submission respecting the review of the Freedom of Information and Protection of Privacy Act, or, as I will refer to it, FOIPPA. I believe you've all been provided with a copy of our joint submission dated June 23.

With us today also, as you noted, are our legal counsel, and that's primarily because our submission surrounds a somewhat technical legal issue, and it may well assist us to have their answers to some of your questions.

Our intention this morning is to highlight for you the impact of a Court of Queen's Bench decision that ruled on the interpretation of section 4(1)(d) of FOIPPA, which led to the recommendations we've made to this committee concerning amendments to the act.

At the end of my presentation the Auditor General, the Ethics Commissioner, and the Chief Electoral Officer will in turn provide some practical examples of the impact of the court's decision on each of their offices. If myself, the other officers of the Legislature, or general counsel are needed, we'll also be pleased to respond to any questions.

The judgment of the Court of Queen's Bench of Alberta dated September 22, 2009, arose from the judicial review of a decision of an adjudicator appointed under FOIPPA who made a decision regarding a complaint made under FOIPPA against the Information and Privacy Commissioner about disclosure of personal information. Section 4(1) of FOIPPA excludes certain records from the act. These include in section 4(1)(d) records that are created by or for or in the custody of or under the control of officers of the Legislature where those records relate to the exercise of the officer's functions under an act of Alberta.

Prior to the Court of Queen's Bench September 2009 ruling it seemed clear that the intent of FOIPPA was that the officer's records were absolutely exempt from the operation of FOIPPA provided they related to our statutory functions under our enabling legislation. For example, my duties as Ombudsman under the Ombudsman Act include the investigation of complaints into the fairness of government actions, omissions in decisions, and the subsequent reporting of my findings and recommendations to the government authority, the complainant, and, in some cases, the Legislative Assembly. Any records generated as a result of an investigation and subsequent reporting would fall within records related to the exercise of my functions. These records can be distinguished from records that

relate to the administration of my office, which would include employee records, contracts for equipment and services, office supplies, equipment purchasing, and budgets, which we have always interpreted as being subject to FOIPPA.

The reason for excluding these records from the application of FOIPPA is not about the officers of the Legislature wanting to protect our turf or avoiding duties or legislative constraints with respect to disclosing personal information. Each of our enabling legislation already specifies what information we have access to and what records we must produce to fulfill our legislative mandates. The legislation also specifies our duties for maintaining confidentiality or secrecy over information acquired and what information must or may be reported to the Legislative Assembly. It makes sense that the legislators explicitly carved out our records from the application of FOIPPA given the unique role that the officers of the Legislature play in the public accountability process.

I reiterate that not all records of officers of the Legislature are excluded from FOIPPA. Each of our offices is a public body under the act. We interpret section 4(1)(d) to mean that records relating to the administration of our respective offices are still subject to FOIPPA. The effect of the Court of Queen's Bench judgment is that officers' records that relate to our statutory duties are still exempt from part 1 of FOIPPA, which relates to requests for information, but those same records will be subject to the protection of privacy provisions contained in part 2 of FOIPPA. In other words, complaints can now be made against each of the officers respecting the disclosure of personal information, and we are now subject to the authority of the Information and Privacy Commissioner.

There are serious implications arising from this interpretation not only for officers of the Legislature but for others whose records are covered by the section 4(1) exceptions to FOIPPA. This section includes certain records of MLAs, Executive Council members, the office of the Speaker, the Court of Appeal, the Court of Queen's Bench, provincial court judges, Court of Queen's Bench masters, and justices of the peace. This interpretation could seriously hinder our ability to candidly report to the Legislative Assembly and to Albertans, thereby weakening the accountability roles assigned to each of us.

Officers of the Legislature may need to appropriately disclose certain information in order to report effectively as authorized by our respective legislation. The court's interpretation will result in conflicts between each of our respective enabling legislation and FOIPPA regarding disclosure of information where no conflict previously existed. As I mentioned in my introductory comments, the other officers will provide concrete examples of this.

Information that we currently disclose in reports as authorized by our legislation could be the subject of a complaint to the Information and Privacy Commissioner under FOIPPA and therefore subject to all of the investigative and inquiry processes under the act and ultimately the courts on an application for judicial review. Not only is the legislative conflict a serious issue in itself, but there are also significant resource implications for all the officers of the Legislature in terms of personnel and costs associated with FOIP investigations, inquiries, and court actions.

11:00

Officers of the Legislature are accountable to the Legislative Assembly and must be and must be seen to be independent of the government and of each other. This independence could be compromised if the other officers of the Legislature are directly subject to the jurisdiction of the Information and Privacy Commissioner and, thereby, subject to the jurisdiction of the courts. Because, in our view, the court did not provide a clear rationale in deciding that only the protection of privacy provisions in part 2 of FOIPPA apply to all of our records, we are concerned that the court's interpretation could easily be expanded in future cases to the request for access provisions in part 1 of FOIPPA, resulting in all of our records being FOIPable, which would be in direct conflict with the secrecy and confidentiality provisions contained in each of our respective enabling legislation.

As the Information and Privacy Commissioner advised in his presentation to this committee in July, the Court of the Queen's Bench judgment has been appealed by the commissioner to the Alberta Court of Appeal, and the other officers of the Legislature have been granted intervenor status in that appeal. The hearing is set for November 3, 2010. In the meantime the records of the officers of the Legislature and those other parties listed in section 4(1) of the act are no longer exempt from the operation of part 2 of FOIPPA, and there is no knowing what the Court of Appeal will decide. Should the Court of Appeal agree with the Court of Queen's Bench interpretation, then unless FOIPPA is amended, the only alternative is a further appeal to the Supreme Court of Canada.

We have therefore recommended that section 4(1)(d) of FOIPPA be amended to expressly exclude from the application of FOIPPA records of the officers of the Legislature except those related to the employment and remuneration of employees of the officers of the Legislature and matters of administration only arising in the course of managing and operating the offices of the officers of the Legislature, including contracts for equipment and services.

We believe such amendments would satisfy the principles of openness and transparency while considerably strengthening the protection of the integrity and privilege of our offices, which is critical to preserving and protecting the public interest that the officers serve. The members of the committee would also be clearly signalling the legislative intent of section 4(1)(d) as it is presently worded; in other words, maintaining the status quo and the legislative harmony that currently exists between each of our acts and FOIPPA.

We trust that our comments today along with our joint written submission will assist this committee in the course of conducting its review and, in particular, highlight for the committee the need for clarity in regard to the exclusion from FOIPPA of officers' records that relate to our statutory duties.

I'll now invite the other officers to provide the committee with examples of the impact of the Court of Queen's Bench interpretation of section 4(1)(d) on each of their respecting officers, maybe starting with Mr. Saher.

Mr. Saher: Okay. Thank you very much, Gord. As members of the committee know, I recently became the Auditor General. I thought I understood the relationship between my act, the Auditor General Act, and the FOIP Act, understood it because of the logical harmony between these two pieces of legislation and appreciated that as a leg. officer I am not above the law. I thought I understood the balance between rights to privacy and the public interest. Our office has always made it our duty to balance those interests and report responsibly every time we issue a public report to the Assembly.

My job is to provide the Assembly with the information it needs to effectively perform its role, but if my reports are subject to FOIP, it could make it difficult to meaningfully demonstrate weaknesses identified and why improvements are needed. For example, we have reported on matters such as executive compensation, severance packages, personal interests conflicting with professional responsibilities, and potentially fraudulent activities. All of these activities

that I've just mentioned: in essence, although we're dealing with systems, at the heart of the issue will generally be an individual or individuals.

For example, I very quickly looked through some past reports. Just to remind you of what I'm talking about, this is a report of the Auditor General, November 2006. The issue was contracting practices at AADAC. Our report started, "From January 1, 2004 to September 15, 2006, a senior AADAC employee . . . through the use of five false contracts, diverted AADAC funds . . . to himself and . . . to other parties." I think we'd have been unable to report on that issue if I was in some way constrained from identifying the individual who was the subject matter of that activity.

The second one – and these were just picked literally at random – a report of the Auditor General of Alberta, April 2008. The subject matter was identifying and managing conflicts of interest for contracted IT professionals. That report started with us writing, "We received a public complaint about a Project Manager at the then Ministry of Infrastructure and Transportation." The subject matter of our work was introduced by identifying publicly that the complaint was about an individual.

Recently we've talked about compensation arrangements at the University of Calgary with respect to the former president of that institution. We also have reported publicly about severance payments as the former RHAs were merged into Alberta Health Services. Those are three concrete examples that my colleague referred to in his introductory comments.

It's not simply a matter of not naming names since personal information goes far beyond that and can meet that definition if the information is sufficient to identify an individual. This is not to say that I'm entitled to disclose personal information freely. I only disclose the information necessary for me to effectively fulfill my mandate.

The reason that I need the clarification of the intent of the FOIP Act is unfettered ability to perform my responsibilities and, importantly, to avoid expensive processes to confirm what has always been the intent. Those expensive processes are – I want to make it clear that I'm not going to not execute my mandate as I think it should be executed and, where necessary, name the individuals that I believe should be named, but with the issue at hand I will have to consume resources. My legal counsel will have to work extra hard in examining whether or not we're doing something that is more or less likely to generate a complaint. All of that, in my opinion, is an unnecessary use of resources with respect to legislation that I believe – at least I believed up until recently – was perfectly clear.

In summary, I'm here today to make the point that what was thought to be clear is clearly not. The purpose of our submission is to bring clarity; it is certainly not to create a new view of life.

Thank you.

Mr. Button: Mr. Chair, having been notified that our time for presentation is nearing an end, the Ethics Commissioner and the Chief Electoral Officer have other concrete examples of the implications of this, and perhaps, if it would be agreeable to the committee, they could present those to you in writing so that they form part of the committee's material, and we can move on with the question period.

The Chair: By all means. It may well be that you can incorporate some of them into some answers for questions that you may also have from some of the members.

Mr. Button: Thank you.

The Chair: If we could proceed with some of the questions, then. I have Mr. Olson.

Mr. Olson: Thank you very much for the information. I have my own view on this, but I'd be interested in whether or not there's been any discussion within your offices about passing some legislation which you would see as clarifying the issue in the midst of litigation on it. I think that we absolutely have the power to do that, but I'm just wondering whether there's been any discussion about that issue, that question.

Mr. Button: We've certainly discussed that issue. We feel that putting ourselves in a position of waiting for the courts to make a decision leaves us vulnerable to a decision which would adversely affect us, as we've laid out in our submission and in our presentation today, and feel that the appropriate and proper thing to do is to bring the matter forward, get clarity on the legislation so that we're not dependent on this ruling or future rulings of the courts to determine what the legislators intended when the legislation was created. When I speak of the legislation, I'm speaking of the FOIP Act as well as the enabling legislation for the four of us.

11:10

To not move forward and act would leave us in a vulnerable position. As you well know, it's difficult to predict where the issue may end up legally, and if we require a clearer interpretation so that the application is quite clear to everyone, then the appropriate thing to do is to make sure the legislation is clear.

I don't know if legal counsel have any other – no?

Mr. Wilkinson: Mr. Chair, something to think about. I guess we all feel this way, but I don't want to speak for them. Certainly, this is the way I feel. It's the end of my presentation. It's just one sentence, and it's something for all of you to think about. Would that mean that members and senior officials who we see are no longer able or willing to make use of our office to identify and avoid conflicts of interest? Is that a distinct possibility?

The Chair: Ms Blakeman.

Ms Blakeman: Okay. As part of your presentation you have stated that the officers are accountable to the Legislative Assembly. My question is that if an individual had a complaint about the handling of their personal information by any of the officers, is there a process that exists currently that an individual could use to bring that matter before the attention of the Legislative Assembly? You've identified the route. Does it actually exist?

Mr. Saher: If it's all right, I'm going to ask Kerry Langford to answer that question, if you don't mind. I think we've had that discussion whereas essentially, if we're not above the law, where does a member of the public have the right – if, for example, named in one of my reports, where would that individual go if he or she felt that that was inappropriate?

Ms Blakeman: Well, specifically, you have referred to yourselves as officers of the Legislative Assembly and accountable only to the Legislative Assembly. What flows from that is that if an individual has a complaint, how do they access that same system that you've referred to? What is available for an individual to bring their complaint forward to the Legislative Assembly? Does that exist?

Ms Langford: I'm not aware of any specific process. In my view,

it would be the Standing Committee on Legislative Offices who has oversight of the officers of the Legislature. As with any other matter in which they were potentially exceeding their mandate and acting outside the scope of the legislation, I believe it would be appropriate, possibly, for an individual to seek remedy through a complaint with the standing committee. Ultimately, it's the Legislative Assembly that appoints the officer, and if there is just cause – for example, again, acting outside their mandate – then it would be up to the Legislative Assembly and the remedies that are available to them to deal with the legislative officer.

Mr. Wilkinson: I think it's a good question. Certainly, in a report that we might make to the Assembly any individual named there would be contacted, would be part of the process, and they would have an opportunity to state their point of view to us as to whether they should be in the report or not, what ideas they had that should be or not be presented. We would take that under advisement, but nonetheless in the end it would be our decision.

The Chair: Mr. Saher.

Mr. Saher: Yes. If I could just supplement Kerry's answer, the question was if we consider ourselves, which we are, accountable to the Legislative Assembly. So there is that process. I think if I understood the question, the way Kerry answered it is the way I understand it, that the same processes through which I'm accountable to the Assembly would and could be used by an individual to take issue with something I had done. So if my accountability to the Assembly is through the Standing Committee on Legislative Offices, that would be the route that an individual could use to bring forward an issue with respect to how I have executed my duties under my act.

The Chair: Thank you.

Ms Blakeman: If there are no additional questions, I'll put myself back on the list.

The Chair: We've got a couple more.

Ms Notley: Well, Ms Blakeman raises a very interesting question, but I suspect we'll have a lot more discussion on it. I was just wondering, Mr. Fjeldheim, if you could give us your most compelling example of where this could be a problem for you.

Mr. Fjeldheim: Yes. Thank you very much. Under the Election Finances and Contributions Disclosure Act we're required to make public those contributions over $375. If this decision is upheld, a contributor or contributors could come forward and say: you're releasing personal information about me and what I have done in making a contribution. In that sense they could complain to the Information and Privacy Commissioner, and then, of course, the election finances legislation that I look after would be in direct conflict with the legislation of the Information and Privacy Commissioner.

Just one more quick one. The list of electors that we've prepared for the administration of the election, of course, is also supplied to political parties, Members of the Legislative Assembly, and candidates. Electors could request that their names not be included on a list sent to a particular party or on lists sent to all the political parties. In that sense that would certainly fetter the party's ability to solicit contributions for the use of the party and its constituency associations and to recruit party members and so on as is contemplated by the legislation. Similarly, it would fetter the members' ability to carry out their duties and functions and the candidates' ability to campaign effectively.

At the polls the list that we would be using for the administration of the election would not be the same as the list that would be held by the candidates and the scrutineers and so on. So there could be, obviously, a big problem there.

Those would be the two that I would like to mention in particular. Thank you.

The Chair: Thank you.

Mr. Groeneveld: How do I get one question in and get the answer here?

I'm assuming that this interpretation caught us all by surprise. Is that correct?

Mr. Button: That's fair to say, yes.

Mr. Groeneveld: Was this red-flagged that this could happen? Or has this just kind of caught everyone with an interpretation that I wouldn't say was off the wall, but it certainly, obviously, was detrimental for you people.

Mr. Button: I would be actually, I think, speaking on behalf of the Information and Privacy Commissioner to answer that in any detail. Brad might be able to add to that.

Mr. Odsen: Thank you. Yes, if I may. This initial decision by the adjudicator flies in the face of all previous decisions in every other jurisdiction in Canada. I think it's fair to say that, no, it wasn't red-flagged, because the representatives of the office of the Information and Privacy Commissioner had no inkling whatsoever that there was going to be a decision coming forth which, as I say, clearly flies in the face of all precedent that exists in Canada with respect to the same legislation. It's an issue of jurisdiction. In essence, the adjudicator determined that notwithstanding that that section says that the records are not part of FOIP, he said: well, they are; therefore, I have jurisdiction, and I can now consider this matter.

All other jurisdictions in Canada have interpreted that same section, where it exists in their legislation, to say: "There is no jurisdiction for the adjudicator to consider the matter. That's the end of it. If it needs to be dealt with, it needs to be dealt with by some other mechanism." Of course, the mechanism that Ms Langford outlined to you is that if an individual has a complaint, they can go to the standing committee with that. They can undoubtedly go to their MLA and have it brought forward by their MLA to the standing committee or, indeed, into the Legislative Assembly itself, I would suggest. Does that satisfy the . . .

Mr. Groeneveld: Can I have a baby supplement here? I'm assuming now that this is going to impact your budgets or has the ability to impact your budget of what could happen down the road.

Mr. Odsen: I think it does. We don't know at this point what that might mean, but certainly we could see much more in the way of legal costs for all of our offices. There may be other resourcing kinds of costs that arise as well in relation to it. So, yes, I think there is no question that it could.

The Chair: I have a question. I know that it will come back to what we have been asking, but mine is quite a bit different. I don't know if it would be the Ethics Commissioner or the Auditor General.

11:20

Those members of the Assembly that are involved in agribusiness are restricted in insurance coverages because in this province we have one crop insurance operation. The Agriculture Financial Services Corporation operates crop insurance, and they have a product called hail insurance. At the end of the year anyone unfortunate enough to have substantial hail damage done to their crop who happens to be a Member of the Legislative Assembly – and there are probably eight members – has those proceeds reported as payments to the MLA. They understand that it's not part of their salary, but I can assure you that a lot of times the public seems to think that somehow they're getting special treatment or that these are additional monies.

I'm just wondering, because it is something that's available to all agricultural producers, why it is that only MLAs who happen to be in agribusiness who happen to have hail claims – and they pay their own premiums for it – have to have this proceed reported in the selected payments to Members of the Legislative Assembly.

Mr. Wilkinson: Mr. Chairman, we have had this discussion. It's a good question and a good comment. Presently that is the way it is because it's reported on the disclosure statement, and then it's made public, as you know. When the act is reviewed in two years, that may very well be something that you want to bring up. You know, whatever your direction is, of course, we'll follow.

The Chair: Folks, time has flown by. We really appreciate the fact that you've presented written submissions as well as being here today to present orally, and we thank you for your time.

Mr. Button: Thank you.

The Chair: Our next presenters will be the Alberta Press Council. While they're setting up, I'd like to ask Mrs. Forsyth: were you able to hear the legal counsel's comments adequately, Heather?

Mrs. Forsyth: No, Barry. I think it's important that they speak in the mike. What they say I am picking up with some of the members when there are questions. They must move up to the mike and then move back or something.

The Chair: Yeah. We had the mike set up at the back room there for legal counsel – Heather, I apologize – and they were trying to rectify it. We'll see if it can be better served in the future here.

Mrs. Forsyth: Okay. Thanks.

The Chair: As with the others, we'd like to welcome you, the Alberta Press Council, in making your presentation to the standing committee here. Before we go any further, we're going to ask you to give us your full name and your title for the record, and then we'll introduce ourselves to you as well. Please proceed.

Ms Mackay: Thank you. My name is Bauni Mackay. I'm the chair of the Alberta Press Council. With me today is Colleen Wilson, who is the executive secretary-treasurer of the Alberta Press Council.

The Chair: Good morning.

Ms Blakeman: Good morning, and welcome to both of you. My name is Laurie Blakeman, and I'd like to welcome you to my fabulous constituency of Edmonton-Centre.

Ms Notley: Hi there. My name is Rachel Notley, and I'm the MLA for Edmonton-Strathcona.

Mr. Vandermeer: Good morning. I'm Tony Vandermeer, MLA for Edmonton-Beverly-Clareview.

Mr. Groeneveld: George Groeneveld, MLA for Highwood.

Mr. Lindsay: Good morning. Fred Lindsay, and I'm from the fabulous constituency of Stony Plain.

Mr. Elniski: Doug Elniski, MLA, Edmonton-Calder.

Ms Pastoor: Bridget Pastoor, Lethbridge-East and deputy chair.

The Chair: I'm chair. Barry McFarland from Little Bow.

Mrs. Sawchuk: Karen Sawchuk, committee clerk.

Mr. Quest: Hi. Dave Quest, Strathcona.

Mr. Olson: Hi. Verlyn Olson, Wetaskiwin-Camrose.

Dr. Sherman: Hello. Raj Sherman, Edmonton-Meadowlark.

Dr. Massolin: Good morning. Philip Massolin, committee research co-ordinator, table officer, Legislative Assembly Office.

Ms LeBlanc: Stephanie LeBlanc, legal research officer with the Legislative Assembly Office.

Ms Lynas: Hilary Lynas, director of access and privacy with Service Alberta.

Ms Mun: Marylin Mun, assistant commissioner with the office of the Information and Privacy Commissioner.

The Chair: Well, now that we've introduced ourselves, we invite you to . . .

Mrs. Forsyth: I'm Heather Forsyth, Calgary-Fish Creek.

The Chair: Heather, I'm sorry. I've done that twice to you now this morning. It's just hard to get used to looking up towards the sky; I'm forgetting that you're there.

Mrs. Forsyth: Well, it's sunny in Calgary finally, Barry, so thank you.

The Chair: Ladies, if you don't mind proceeding with your 15-minute presentation, leaving us time, hopefully, for some questions for you.

Alberta Press Council

Ms Mackay: Thank you very much, Mr. Chair. We really appreciate this opportunity to address this committee. Ms Wilson will help answer questions when I'm done my presentation. Before I begin, however, I do want to point out that the Alberta Press Council is a nongovernmental, nonprofit, volunteer organization representing the 109 weekly newspapers that are members of the Alberta Weekly Newspapers Association as well as five daily newspapers: the *Edmonton Journal*, the *Calgary Herald*, the Red Deer *Advocate*, the

Lethbridge Herald, and the Medicine Hat *News*. The council is composed of both public and press members.

This review of the Freedom of Information and Protection of Privacy Act is timely and of great interest to the Alberta Press Council. A primary part of the Alberta Press Council mandate is to promote and protect the established freedoms of the press. Inherent in this mandate is advocating freedom of information. It is this aspect of our mandate that fuels our interest in the Freedom of Information and Protection of Privacy Act, on which I would like to focus today.

Because you have the written submission that we sent to you a few weeks ago, which includes our concrete suggestions for reforms to the Freedom of Information and Protection of Privacy Act, I won't repeat what we said in that submission. Instead, I would like to dwell on the connection between freedom of information and freedom of the press and the inherent implications of this connection for our democratic system of government.

Press councils around the world share our concern about the erosion of press freedoms, transparency, and independence of information. It is interesting to note that in a world where even in democratic countries information is often censored, filtered, or withheld, Iceland has just instituted the modern media initiative and plans to become the global haven of journalistic freedoms. It is also interesting to note that based on the free flow of information, the Freedom House world audit ranks Canada 17th in press freedom among 150 countries with populations greater than 1 million.

Freedom of information is a basic human right. Article 19 of the Universal Declaration of Human Rights states:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Yet the fundamental principles of freedom of the press here and elsewhere are more threatened today than at any time in the recent past due to the barriers that prevent or dissuade accessing information that is substantive, complete, timely, and affordable.

The right to freedom of information should be especially sacred in a democracy because a well-informed citizenry is the foundation upon which the democratic system is built. To impede the flow of information is to diminish democracy. To enhance the flow of information is to strengthen democracy. Yet in a world where the desire for instant access necessitates speed and superficiality, where the sound waves, airwaves, and cyberworld are polluted with the minuscule details of the transgressions of entertainers and sports heros, where talk shows and social media have replaced thoughtful discourse with sensationalism and inane babbling, this fundamental, tentative democracy is threatened. In a world where more time and money are spent on public relations than on factual research, where spin has replaced truth and managing information has replaced honest disclosure, even conscientious citizens allow themselves to be manipulated.

We are bombarded with information, often at breakneck speeds, but the sheer volume and questionable quality of that information serves as a distraction from what is important and diverts us from the critical thinking, probing curiosity, and vital engagement that are necessary to sustaining a sociopolitical system that is transparent, accountable, and democratic. Because accountability is not possible without transparency, it is the aim of newspapers to keep readers informed on matters of public interest and concern.

By providing in-depth, fact-driven, investigative reporting, newspapers deliver complete, accurate, and reliable information that citizens depend on to make informed choices on matters of public interest. In the absence of disclosure of material related to the development of public policy, the public depends on the press to use freedom of information processes to discover matters of public interest related to the performance of public bodies and to the development of public policy. Otherwise, the press and hence the public are increasingly reliant on news management as demonstrated through leaks, public relations, and spin-doctoring.

11:30

Newspapers are unique among the news media because they are able to do what sound bites and video clips cannot: use the printed word to expand, develop, and embroider a story with details that only they have the capacity to research and the space to include. Traditionally newspapers have had the luxury of time and space that the electronic media – that is, radio and television – have not. However, the newspaper industry is changing. In order to compete with the instant-access media and in order to survive in the digital world, newspapers have had to respond to the economic environment in which they find themselves. This means they, too, have gone digital, some more than others, and immediacy has become even more critical.

The economic environment also means newspapers often work with a less than full contingent of staff so that digging for information has to be done by fewer people in less time. Ironically, providing the newspaper reader with in-depth investigative journalism has become increasingly difficult in the information age; therefore, allowing journalists to access information efficiently and economically has become even more important than it has been in the past.

Because public bodies often block access through exemptions, time delays, and excessive fees, some journalists make little use of the freedom of information processes and instead find it easier and quicker to acquire information via unofficial leaks and off-the-record briefings. Without access to source material journalists and their readers are subject to spin doctors, who tell only their side of the story. This makes journalists more vulnerable to being manipulated and misled and thus makes it easier for public bodies to manage the news. This, of course, erodes the democratic process.

Changes to the freedom of information and protection of privacy legislation in Alberta can do much to expedite the complete, accurate, and reliable transmission of information from public bodies and thus enhance the transparency and accountability of those public bodies. For purposes of investigative journalism the value of information reduces in proportion to the time it takes to acquire it. The significance of the story is often lost by the time the information is acquired, so essentially access delayed is access denied.

The increasing use of private contractors discourages the flow of information, and the act should require that anybody paid from the public purse, directly or indirectly, be subject to the act. By providing adequate resources and training, the government would increase the probability that freedom of information applications are processed in a timely way.

There is a need to encourage the development of an ethos within the public service and government which is consistent with the notion that the public has a right to be informed. Secrecy must not be an automatic entitlement. It must be justified based on true appreciation of the harm that would result in its absence. Demands for secrecy should be overridden where the public interest outweighs the risk of embarrassment or inconvenience to a public body. Often the information labelled as the most sensitive by public bodies is the very information that is most critical to the accountability of that public body. Exemptions to the disclosure of information should be limited only to those that are harmful to the public interest, but even within exemptions there should be discretion as to whether or not to release information.

In our view the act should be reformed to make the suppression of information of public interest and concern much more difficult. It should be an offence to withhold information improperly or for an inappropriate purpose. Unjustified delays and unreasonable fees should also be classified as violations of the act because these, too, are barriers to information and thus impediments not only to maintaining the established freedoms of the press but also to sustaining a strong democracy.

I wish you well in your deliberations and am hopeful that the review of the Freedom of Information and Protection of Privacy Act will ultimately result in easier and fuller access to information by all Albertans, especially those who read newspapers. I'll answer questions.

The Chair: Thank you very much.

Our first questioner is Ms Blakeman.

Ms Blakeman: Thanks. I want to thank you for your submission. It was very clear and contained a number of examples that are helpful to me as a committee member in understanding where some of the problems have arisen. I think you're onto something with identifying the issues around third-party vendors or third-party keepers of databases, and I want to concentrate on that. I think we're all familiar with those software programs where you hit "agree" or don't get the information. It's an all-or-nothing situation. I'm wondering if you have any information about contracts that have been negotiated with public bodies that limit the ability to provide access. I'm looking for specific examples of where someone in the newspaper sector has tried to get information and has been told: "No. The information is now in this database. It's third party. You can't get at it."

Ms Mackay: Well, I'll give you an example from the reporter at the *Edmonton Journal* who gave me the example to show me what this meant because I didn't really quite understand it. For example, in a group home which is funded by Children and Youth Services, the people who run those group homes are not subject to giving the same information that maybe the department would. I mean, they're protected because they're private and they're a third party. So there would be an example.

Ms Blakeman: Are you aware of situations where a third-party software company or a database holder has refused to sign a contract with a government or public body that says: you have to give us the information?

Ms Mackay: I can't give you a specific example, but this again came from a *Journal* reporter, who said that she has had difficulty in accessing information. The way she described the situation was that it's like giving somebody else the filing cabinet with all the information in it and then giving them the key to it as well and not having other people be allowed to access it. That would be the only example I could give you because, of course, as the Press Council we don't deal with the specifics of that kind of thing unless it comes to us as a complaint. To my knowledge there hasn't been a complaint, but Colleen maybe can give you another example.

Ms Blakeman: If you can get us examples back from those same reporters that sourced this to you, that would be helpful for us to understand how much of an issue this is or how many times it happens.

Thank you.

Ms Mackay: Okay. We can do that.

Thank you.

The Chair: Ms Notley, did you have a question?

Ms Notley: No. I wasn't on the list.

The Chair: Mr. Quest, then.

Mr. Quest: Thank you, Mr. Chair. Just towards the end of your submission here, top paragraph on page 2: exemptions to the disclosure of information should be limited only to those that are "harmful to the public interest." I'm just wondering who would decide what is harmful to the public interest, and maybe get an example.

Ms Mackay: Well, I think that's probably where you get into the privacy issues. I think all of us want to protect our privacy. I mean, if you could go willy-nilly giving information about kids who are in care, for example, that would be harmful to the public interest. That is not in the best interests of those children. It's also not in the best public interest to have that much openness in a situation, I guess, so that could be an example.

Meanwhile, within that there should be situations where information that is suppressed, that would have absolutely no – I mean, it is in the public interest. It is not harmful to the public interest, but often it is still not accessible for reporters. Here's an example I guess I could give you. When children in care – I don't know why I'm picking on this particular department; it's just because that happens to be in the news quite a bit – are hurt or murdered, which we've had a few cases of, that child's name is not ever identified. I guess that's the question. Should it be, given that: who are you protecting at the point in which the child is dead? Who are you protecting? Maybe the people of the province would like to know who this little person was that walked the Earth for two years and then was murdered or whatever.

I think the thing is that sometimes these things are shaded by not being in the public interest, yet sometimes maybe there have to be doors opened so that some of these things can be identified.

11:40

Mr. Quest: Okay. All right. Thank you.

The Chair: Thank you.

Ms Pastoor.

Ms Pastoor: Yes. Thank you. I think that we probably all understand that we receive information in electronic format and that it really is very convenient and quick and all of that. Could you explain your proposal for an open data provision in the act? Just what does that mean in terms of: opposite to the electronic format?

Ms Mackay: I didn't use the term "open data," so I don't know what you're referring to.

Ms Pastoor: Well, if I'm understanding it correctly, the open data would be information that I think would already be available. People would provide more, I guess, on the Internet, and you'd be able to just go in and get it.

Ms Blakeman: The city of Edmonton does that now. They use open data sourcing for a lot of their information. For example, bus schedules are available. They publish them online. As a result

you've got the Google maps, that can give you very good directions on when a bus is coming and where to catch it. So it's providing raw information on the Internet that somebody can then search through themselves rather than the finished product only.

Ms Mackay: Yes. I think that that's the thing that newspaper reporters are often frustrated with, that they can find the information as it has been presented publicly in whatever format. Bus schedules: obviously, those are accurate. But sometimes the access to information that they get has already been managed in that it's somebody's point of view or some things have been left out or whatever. What they would like is raw data so they can look at the spreadsheets, can draw the conclusions, can write the story from a very objective point of view rather than having to look at the finished product after someone else has manipulated it, perhaps. That's too strong a word, but I can't think of another one right now.

Ms Pastoor: That's fine. Thank you.

Dr. Sherman: On the fees. Can you suggest what fees would be reasonable to allow you to do your job, and what are reasonable timelines? We heard from the previous group that they wanted an emergency time of 48 hours to get the information so they can report. What would be your suggestions?

Ms Mackay: Okay. I know. You're looking at the submission that I gave you two weeks ago or three weeks ago or whatever it was – right? – rather than the one I've just made. That's why I'm kind of floundering here to see where these questions are coming from. [interjections] Oh, okay. All right.

Well, I think that in our submission from a few weeks ago we did talk about fees as well and said that fees are often exorbitant when they're being charged by the public body that the reporters have gone to. One example that was given was the amount of money that was going to be used to get the information relative to the restaurants and the situation in the restaurants when they were trying to do a story on which restaurants had violated the health act and so on. We wouldn't have a suggested price. In this case the commissioner actually said that that information should be free, that there should not be a cost to it. I think most newspapers, the big newspapers anyway, are probably willing to pay something. It's when they come up to thousands and thousands of dollars that they're expected to have to pay, supposedly to take care of the administrative costs involved in getting this information to them. That's where things fall apart. Obviously, newspapers who don't have money can't even afford to do that, and the ones who can afford it question it because they, too, have other places they could be spending their money. But I can't give you a number.

Dr. Sherman: Thank you.

Mr. Olson: Well, I'm also interested in the fees. By the way, thank you very much for a great presentation. On the question of fees, I think we're all looking for a balance between, you know, reasonable access at a reasonable price without creating too much of a burden on a public body so they're having to bear a lot of the cost.

One of the things I notice. Now, this is not from your submission today but from the one that we got previously. You cite a number of examples, and the fees are horrifying, but in every example you gave, I think, ultimately they were refunded or somehow overridden by the commissioner, whatever, which suggests to me that, you know, possibly the system is kind of working. I'm just wondering if you could comment on whether you think it would be reasonable that maybe there be some sort of a maximum fee that could ever be charged to try to keep both sides honest somehow. What we hear from the public bodies is that they're sometimes repeatedly asked for information and stuff, so they're having to use a lot of resources to try to provide that information.

Ms Mackay: Yes, and of course that all makes sense. I think that if there was a maximum set, that would certainly be a step in the right direction. The problem with newspapers, of course, is that everything is time sensitive. While they worry about, you know, how much this is going to cost, when they get struck with something that says, "You're going to pay $300,000 to get this information," then everything stops. They have to make the decision: do we go ahead and pay it, do the story, and then go to the commissioner? The process doesn't work fast enough for it to be very expedient in terms of getting the news out. That would be the issue as much as the money itself.

The process may very well be working. Certainly, in these cases that we gave you as examples in the last submission, they did work in terms of what the commissioner came up with, but by that time, you know, the story would be long dead. Right? That's probably the main issue.

If there was an absolute maximum and the newspaper would know when they tried to do this research that they could be charged as much as whatever that fixed is, then they can be prepared to do that. They can still fight it if that's what they choose, but they would at least know what that would be. I think that in this case, when it was the $300,000 or something they were being asked to pay, it was just, you know, so out of the ballpark that it really stymied them for a while, and it undoubtedly affected the quality of the story in the end.

Mr. Olson: Okay. Thank you.

The Chair: Thank you, Mr. Olson.

Now Ms Notley.

Ms Notley: Well, yes. I was just going to actually carry on on that very same topic. I guess my question, depending on whether you have the answer, challenges perhaps the characterization by Mr. Olson in that, you know, if the system corrects itself two years later, then in fact what's happened is that the price estimate has been used very effectively as an impediment, depending on whether the requester is someone who can afford to roll the dice on $144,000 and fight that fight afterwards. My question is: in the two cases that you cite there, where these prohibitive fees, which were clearly designed to be another way to say, "No, we're not giving you that information," were ultimately waived, what was the timeline? How long did it take for those fees to be waived, and if you don't know, could you let us know?

Ms Mackay: Yeah, we can let you know. I don't know the timeline. I just know it was significant enough that it did affect the story, and it was the reporter who was doing the story who was giving us this information.

Ms Notley: I definitely appreciate the timelines and the issue of deadlines that the press deal with. Above and beyond that, it may still be valuable to a member of the public a month or two or three months down the road, but, you know, it really depends on how long it takes to get an answer on whether these types of ridiculous fees are going to be waived. If you could let us know after the fact, that would be really helpful.

Ms Mackay: We will. Thank you.

The Chair: Thank you.

Ms Blakeman: You've made two really good recommendations in here that I think would be helpful, certainly, to those of us in the opposition, who are seeking information from government, that share a lot of the same challenges as the media sector does in trying to get information. One is the listing of databases that would contain information so that we can accurately ask for the routing, if I can put it that way, and the second is that the records management policy be posted online for various departments. I think those are great recommendations because it helps us as requesters of information to be more specific to the government bodies so that we can't be put off so easily. Do you have examples of where this is in place somewhere else in the world that we could look at? If we were trying to adjust the act and we're looking for wording, do you know of any other place that this might already be in existence?

11:50

Ms Mackay: I don't right now. I suspect Iceland will be one of the first places that will do it. That's the whole point I referred to in my remarks today. The whole point of that initiative is to have the databases even from countries where, you know, information is suppressed much more than it is here. They would have that kind of information in their database so that it could be accessed by reporters around the world. In fact, that would be a website I would certainly recommend that this committee look at because they're really on the cutting edge of recognizing that connection between freedom of information legislation and freedom of the press.

Ms Blakeman: I'll ask you to send that information through to the clerk because I think our time with you is over.

Ms Mackay: Okay. I will.

Ms Blakeman: Thank you.

The Chair: On behalf of the committee we'd like to thank you for making your presentation and making yourself available to us today.

Ms Mackay: Okay. Thank you.

The Chair: Committee and staff, we're now adjourned until 12:45 for lunch. I would ask you to be here promptly because our presenter after lunch is on teleconference. We'll be hooked up and ready to go at 10 minutes to 1. Our lunch will be served across the hall.

[The committee adjourned from 11:51 a.m. to 12:49 p.m.]

The Chair: Good afternoon. Welcome to the afternoon session of our review. This afternoon we have the B.C. Freedom of Information and Privacy Association. Our next two presenters are participating via teleconference. I'd like to welcome Mr. Stanley Tromp to our meeting.

Mr. Tromp, before you begin your presentation, our members and staff are going to introduce themselves to you and for the record. We'd also like you to give your name and position for the record down here, please.

Mr. Tromp: Thank you.

The Chair: Ms Blakeman.

Ms Blakeman: Thank you.

Via the airwaves welcome to the meeting. My name is Laurie Blakeman, and I am most honoured to be the MLA for the fabulous constituency of Edmonton-Centre.

Ms Notley: Hi. Welcome, sort of.

An Hon. Member: Sort of?

Ms Notley: Well, you're very welcome; it's just that you're only partially here. That's my point.

My name is Rachel Notley. I'm the MLA for Edmonton-Strathcona.

Mr. Vandermeer: Hi there. I'm Tony Vandermeer, the MLA for Edmonton-Beverly-Clareview.

Mr. Groeneveld: Good afternoon, guys. I'm George Groeneveld, the MLA from the district of Highwood.

Mr. Lindsay: Good afternoon. Fred Lindsay from Stony Plain.

Mr. Elniski: Hi. Doug Elniski, the MLA for Edmonton-Calder.

Ms Pastoor: Hello. Bridget Pastoor, MLA, Lethbridge-East, and deputy chair.

The Chair: I'm Barry McFarland, the chair and MLA for Little Bow.

Mrs. Sawchuk: Karen Sawchuk, committee clerk.

Mr. Quest: Hi. Dave Quest, MLA, Strathcona.

Mr. Olson: Hi. Verlyn Olson, Wetaskiwin-Camrose.

Dr. Massolin: Good afternoon. Philip Massolin, committee research co-ordinator and table officer, Legislative Assembly Office.

Ms LeBlanc: Stephanie LeBlanc, legal research officer with the Legislative Assembly Office.

Ms Lynas: Hilary Lynas, director of access and privacy with Service Alberta.

Ms Mun: Marylin Mun, assistant commissioner with the office of the Information and Privacy Commissioner.

The Chair: I won't forget this one. Joining us also via airwaves, out of Calgary, Alberta, is . . .

Mrs. Forsyth: Heather Forsyth, Calgary-Fish Creek. Welcome.

The Chair: Thanks, Heather.

Mr. Tromp: Thank you.

The Chair: Mr. Tromp, you have 15 minutes for your presentation, and then I'll open the floor to questions for you from the committee. If you care to proceed, we'd be happy to hear your presentation.

Stanley Tromp re B.C. Freedom of Information and Privacy Association

Mr. Tromp: Thank you very much, Chair. My name is Stanley Tromp. I'm a freelance reporter based in Vancouver and author of the book *Fallen Behind: Canada's Access to Information Act in the World Context*. I was commissioned by FIPA to write this report on Alberta law, but I'm not speaking formally on behalf of FIPA or any other organization.

Greetings from across the Rockies, hon. members, where it's now about 12 noon. Thank you for this opportunity to speak today.

Your first question might be: why is a group from British Columbia making a submission to Alberta? That is a fair and reasonable question indeed. Well, the B.C. Freedom of Information and Privacy Association is a nonpartisan, nonprofit society that was founded in 1991 to promote and defend access and privacy rights in Canada. Our goal is to empower citizens by increasing their access to information and their control over their own personal information. B.C. FIPA has a long record of concern for Alberta that continues today. In the early 1990s, as the Alberta law was being proposed, B.C. FIPA executive director Darrell Evans was invited to the province by the Alberta Civil Liberties Association to speak at public events on proposing needed FOI measures and educating the public, and he has since returned to speak in fall 2009.

To begin, I was pleased to read in this committee's advertisement for public input that it was seeking suggestions to "modernize the Act" and to "harmonize the Act with other access and privacy legislation" for that is my primary field of study. Most of the discussions regarding the FOI Act reform are by now familiar, so I wish to consider another perspective on the issue, one not explored yet, that we could continuously reframe the Alberta act in light of rapidly changing international and historical context.

Now, although Canada has not yet done so, at least 40 other nations today explicitly grant the public a right to obtain government information in their constitution or bill of rights. Since the mid-1990s there has been a profound shift in the way FOI is understood. At first it was viewed primarily as a governance reform, but now, in stark contrast, FOI is globally seen as a fundamental human right.

In the past decade our knowledge or experience of this subject has multiplied, and we can now draw more accurate conclusions about this. To this end, I created a world FOI chart in 2008 to help FOI scholars and posted it to my website. This Excel chart cross-references key documents on FOI law, including text of 73 national FOI laws, all the Canadian, provincial, and territorial FOI laws, and the commentaries of 14 global and 17 Canadian political organizations. My report compares sections of the Albertan FOI and privacy law with those of other provinces and nations. For readers wanting to pursue the topic further on the world FOI chart, when you scroll down to row 16, you can compare Alberta's FOI Act section by section to all the other laws.

It seems the whole ground has shifted, for a decade ago we did not have clear global FOI standards that each FOI law could be measured against, but now we do, and Alberta could raise its own FOI law up to the very best standards of Commonwealth nations and then look beyond the Commonwealth to consider the rest of the world. If one section of the Alberta FOI Act would be helpful for adoption in other jurisdictions' FOI laws, then why not vice versa?

12:55

Even the United Kingdom, the Canadian parliamentary model, has well outpaced us on many critical points although, frankly, it still lags behind us on a few others. Now, some Canadian officials to put off FOI reform still invoke the great tradition of Westminster-style confidentiality, yet the British FOI law has several positive features absent from the Alberta FOI law such as a harms test for policy advice, a 20-day response deadline, and a 30-year time limit for legal advice records.

On FOI reforms Canadian parliamentarians need not leap into the future but merely step into the present. The best examples for Canada to generally follow for inspiration are, I believe, the access laws of India and South Africa in most but not all of their respects.

There is a familiar objection. Critics call it absurdly naive to presume any such superior FOI laws will be enforced or effect any reality on the ground. These statutes might be just paper tigers, they say, being laws completely ignored or ineffective in actual practice. Well, that is in fact often sadly true. But should these facts discourage us? Yes and no. Although I am fully aware of such objections, I would reply that statutes are comparatively more important and enduring than actual government practices of the day. There are many good FOI laws that do not result in good practice, but one very rarely sees good FOI practice without good FOI law first in place as a foundation for it.

To understand this Alberta law, I have consulted the widest range of sources I could find, the most important being the reports of the 1993 legislative discussion groups, the 1999 and 2002 legislative reviews, and the commissioner's annual reports. I focused on the statute's text, and although the B.C. FOI law was virtually replicated in Alberta, I'm careful not to presume that poor FOI practices elsewhere in Canada also necessarily appear in Alberta. In fact, Alberta has some features in the law that outpace the rest of Canada.

The value of strong FOI law is better demonstrated than just asserted. For your interest I've compiled summaries of 50 news stories on issues as diverse as health, safety, government waste, public security, and environmental risks, stories made possible by the Alberta FOI Act, and posted them at my website. You may have seen them already when I sent the link to you.

Well, there are a number of specific issues here. One serious problem today is that there is a growing trend in Canada towards contracting out public functions to so-called private entities that are not covered by FOI laws. Some are in effect shell companies wholly owned by government. The law needs amendment to clearly state that any public body, any corporate subsidiary of a public body, and any organization that is controlled by a public body or receives its funding primarily from public sources or delivers a public service should be automatically covered by the Alberta FOI law when it is created.

Now, I emphasize that I do not oppose privatization of public functions per se, only the loss of public transparency and privacy protection that often accompanies it but should not. Some governments have granted some of their wholly owned companies exclusions from FOI laws, claiming that they required special protection from the commercial competitors. Such claims are illogical and spurious because the Alberta FOI law already contains generous protections such as sections 16 and 25 to prevent such harmful information releases.

Regarding fees, it is possible that the $25 application fee has discouraged potential FOI requests from very low-income public-interest researchers, students, and alternative media, so it should be eliminated. This dampening effect would run contrary to the democratic intent of the act. Federal Information Commissioner Robert Marleau advised Ottawa to drop the $5 fee to make an access to information request because he estimated it cost $55 to process the $5 cheque. The same general principle likely applies in Alberta. There is no cost to file FOI requests in B.C., Saskatchewan, Manitoba, Quebec, the United Kingdom, and the United States. Perhaps the $25 fee was added to block a truly mischievous applicant from filing thousands of frivolous requests for free, but if

so, such a case would be too rare to design a general principle upon, and if it did ever occur, the government could apply section 55 to block requests that are "frivolous or vexatious."

Even worse in the Alberta act is section 29: a public body may refuse to disclose to an FOI applicant information that is "available for purchase." I cannot quite understand why the question has been missed in the law and its discussions on it: that is, available at what price? Is there to be disregard for the lowest income information seekers? In practice the government could simply charge $10,000 if it wished to as a means of limiting access to a report for some political reason, and the applicant today would have no recourse. Some very highly priced information may be truly in the public interest for readers; for instance, concerning health, safety, and the environment. I advise, as a minimum, amending section 29 to allow the applicant to appeal to the commissioner an information sale price of more than $1,000. The commissioner would not make an order on the matter but could publicly comment on the reasonableness of the price.

To sum up, it was well observed by a prominent Albertan, the current Prime Minister, quote:

> Information is the lifeblood of a democracy. Without adequate access to key information about government policies and programs, citizens and parliamentarians cannot make informed decisions, and incompetent or corrupt governance can be hidden under a cloak of secrecy.

Unquote.

In the same spirit Robert Clark, the first Information and Privacy Commissioner of Alberta, in his submission to the legislative review in 1998 said:

> The Act has had a significant impact on Albertans. It safeguards their privacy, at least with respect to government. It has made the workings of government more visible to the people . . . It has made the government better, because you make better decisions when you are [more] accountable. I would hazard a guess that it is changing the way government deals with people generally because openness and accountability are the hallmarks of fairness.

Finally, it is also noteworthy that on his very first day in office, January 21, 2009, U.S. President Barack Obama issued an executive order to all government agencies to reverse the default secrecy position of his predecessor. A similar public order from the Premier to the Alberta public service would be most welcome. As President Obama wrote:

> The Government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears . . .
>
> All agencies should adopt a presumption in favour of disclosure, in order to renew their commitment to the principles embodied in FOIA, and to usher in a new era of open Government.

Although I've made hundreds of FOI requests, although none yet in Alberta, and have intensively studied FOI theory in statutes, I still do not have all the answers, nor does any single individual or institution, yet I do believe that most of these recommendations may merit consideration. In the end, of course, all the choices remain yours. This subject is one of the most important and interesting you might ever deal with for it establishes the relationship between citizens and their government.

In regard to information access and privacy protection the government of Alberta made a strong start with the passage of its statute in 1994. One can still do more. By raising the Alberta FOI law up to the best world standards, legislators can also greatly enhance their democracy and create a lasting legacy for their constituents.

With the passage of the 79 reforms I've suggested here, Alberta could lead the way in FOI and privacy topics and be an inspiration for the rest of Canada. I would urge you to seize this challenge today.

Thank you for listening. I would be pleased to answer any questions.

The Chair: Thank you very much, Mr. Tromp.

Mrs. Forsyth: Barry, if you could put me on, please.

The Chair: Certainly.

If you want to just wait one moment, Mr. Tromp, we've got Ms Blakeman first, and then we'll have Mrs. Forsyth.

Mr. Tromp: All right.

Ms Blakeman: Thank you very much. I'm very interested in the concerns around service providers under contract. In the submissions that we've had, we've had the Alberta Press Council arguing, very similar to you, that FOIP should clearly apply. The Alberta universities have said that there should be specific obligations spelled out. We've had others like the government and the Privacy Commissioner say that the FOIP Act already applies and that, essentially, a public body cannot contract out its obligations. Can you explain briefly but specifically why an amendment is needed and, in your opinion, how this would affect both access and privacy?

1:05

Mr. Tromp: Well, this is really the most complex subject of all, and I devoted about the first half of my report to it. It's rather confusing, the distinction between what is ownership, custody, or control of records; should an entity be covered by the law itself under a schedule or only the records of that private company; and what constitutes custody or control.

A wholly owned government company, for example, should clearly be covered, but some others are less clear because services are contracted out to an entity that might not be actually owned per se. It is generally a global standard that for whoever provides public services, their records are covered by the FOI law. This needs to be done. There need to be standards set in the statute itself. I have many recommendations in here such as 11, 12, and so forth, and that's to amend section 3 of the act. The scope of the law's coverage should extend, really, to any institution that's established by the Legislature or by any public agencies, even local public agencies, which is very . . .

Ms Blakeman: I'm sorry; I'm just going to interrupt you to clarify here. I understand what you're saying. I've read your recommendations, and I've referenced recommendations 11 and 12. The problem seems to be that some people think it's already in there, and some people think it's not. That's what I was trying to get you to get at: where exactly is the problem? If I'm trying to solve this and pitch to the committee to change something, where exactly is the problem that needs to be changed?

Mr. Tromp: Yes. Well, the problem in the law is that it's not explicitly stated what sort of services should be covered. It's left to regulations and schedules, putting one entity at a time at the government's leisure. You have a recommendation 12. If the wording of that were placed in the law, then that would remove most vagueness about what is covered and what is not. I mean, probably they think it's implicit in the law what is covered, but it's not clear enough. It should be made explicit so there's no doubt or ambiguity what it means. Many statutes do have that such as in Europe and the United Kingdom and so forth. It has to clarify, really, that records created

by or in the custody of a public service provider under contract to a public body are under the control of the public body. It's not necessary that the private entity should itself be covered by the law completely, such as its records on its private business, but only on its public business.

Ms Blakeman: Thank you very much.

Mr. Tromp: There may be some confusion around that.

Ms Blakeman: That's excellent.

Mr. Tromp: Thank you.

The Chair: Mrs. Forsyth, please.

Mrs. Forsyth: Thank you, Chair. I may be following up under something that Ms Blakeman said. It was a statement you made when you were making your presentation about government contracting private bodies who don't fall under the law, and it's sort of a protection from the government. Could you give me an example so I can fully understand what you mean by that?

Mr. Tromp: Well, I haven't studied the Alberta situation very much, mostly the British Columbia situation. If, for example, a private security company guards a city hall or so forth, that is a public duty, and even though it remains a private body, all of its public duties regarding the coverage of city hall should be open to the public under the FOI law but not when it guards private property. Then those duties remain private. That should be explicitly, I think, written into the text even of public-private contracts, that these records of the public duties are subject to the FOI process, because the public really has a right to know what affects them. Even, say, private prisons or private schools and so forth, which are becoming more popular: that is really the public's business.

Mrs. Forsyth: Okay. I'm still a little confused on this. I think probably what you're suggesting, for example: it may be the case in Alberta that under our School Act we have private schools or we have chartered schools, so they would be exempt. Is that what you're saying?

Mr. Tromp: Well, if it's a purely private institution, if it's not publicly funded or having its appointments of its executives by the government, then it would remain private, of course. Yes.

Mrs. Forsyth: Okay. Thank you.

Ms Notley: I wanted to sort of carry on on this because this is an issue that I'm very concerned about. I actually in some ways share Ms Blakeman's questions because we do appear to be getting two different assessments about the availability of information to the public that's held by private bodies that are providing a public service under contract. I was thinking that just because of your expertise and that you appear to have done some studying across the country, can you tell us: has this issue been addressed or discussed in any other jurisdictions in the country?

I mean, we've got documentation here that, at least at this point, it appears as though there's no jurisdiction in Canada that has more clarity on this issue than ours. Everyone seems to be sort of equally unclear in terms of how you deal with the growth of contracting out services. My question is: are you aware that there has been conversation or study or consideration of the issue in any other jurisdictions in the country?

Mr. Tromp: Oh, yes. This is a huge issue across the country, and I predict it may become the single most important issue in the FOI law because if governments can create shell companies to put records away, then who knows? The loss of FOI could spread greatly and become like a vacuum. It's most serious, I think, in the federal sphere because there are at least a hundred quasi-governmental bodies such as the air traffic controllers, the Blood Agency, and nuclear waste management agency that are wholly owned by government, do public services, and are not covered by the federal law. In 2006 the Conservative Party running for office pledged to cover all entities that are doing public service and are owned by government such as that, but they did not do so. They did some but not all of them; that is to say, wholly owned subsidiaries of Crown corporations but not others.

In British Columbia that's becoming a major issue as well. We had a case of the University of British Columbia having three privately owned entities, and I appealed that. The commissioner ruled that those records should be public because they're wholly owned and controlled by the public institution. The university appealed, and that's ongoing.

That's really the major struggle. I mean: what is public, and what is private? You have to stand very firm on the principle that records that deal with public services and the provision of public services also funded by the public should be public records. That is a major problem. However, there are other jurisdictions and countries that are much more up to date in their law about covering these issues and these entities and records than we are.

Ms Notley: I'm sorry. You may have put this in your document, and if you have, that's great. Did you recommend to us a model provision in any other jurisdiction?

Mr. Tromp: Oh, yes. There are several.

Ms Notley: If you did, that's okay. I'll find them.

Mr. Tromp: They certainly are in there, yes, in recommendations 3, 4, 5, 6, and 7, at least going up to 12. That's how large the issue is. It took half my time, actually. It's an ongoing issue. In Alberta it doesn't seem to matter quite as broadly as British Columbia or the federal government, where they seem to create more of these at the present time. But I fear in the future . . .

Ms Notley: You may have misunderstood my question. Other jurisdictions: was it the U.K. or Australia or Iceland? Did you have any recommendations of language that's actually in place that addresses this in other jurisdictions that are worth looking at?

Mr. Tromp: Oh, yes. It's in regard to the scope of the act. I'm just going through my pages here, and there are Canadian provinces. In Manitoba it's the law. In Nova Scotia it's the law. Other nations such as New Zealand and India prescribe FOI coverage for official information held by public bodies, state-owned enterprises, and bodies which carry out public functions. The term "public functions" does not appear in the Alberta FOI law or Canadian laws, which it needs to be in. India is very advanced on this as well. It says that bodies controlled or substantially financed by the government and nongovernment organizations which are substantially funded by the state are covered, as they should be in Canada, too. We've just fallen behind the rest of the world.

1:15

The Chair: Thank you.
Mr. Lindsay, please.

Mr. Lindsay: Thank you, Chair. Mr. Tromp, thank you for your very interesting and comprehensive comments. Would it be accurate to paraphrase your views as philosophical as opposed to based on actual incidents of concern with the legislation here in Alberta?

Mr. Tromp: Well, I suppose. I don't live in Alberta, and I've never filed an FOI request in Alberta, but I've studied it very closely. It was almost a replication of the British Columbia law, which I'm very familiar with, so I just apply it as well as I can.

Mr. Lindsay: Thank you for that. A lot of the legislation, how effective it is, is based on how it's interpreted and carried out in different provinces, so I appreciate your views.

Mr. Tromp: Well, that's true. I've put notes on interpretations, and I've read the commissioner's old rulings and annual reports as well, which are very enlightening.

The Chair: Thank you, Mr. Lindsay.
Mr. Verlyn Olson, please.

Mr. Olson: Thank you. Thank you very much for the information. I just have one quick question. I'm referring to page 26 of your report, where you commend a process that has been developed in B.C. since 2006, the consent order or expedited inquiry, which, as I understand it, involves the agency and the applicant agreeing on a timeline. I'm curious as to how that works. You indicate that it seems to have really worked well in B.C., but is there a struggle arriving at that timeline? Is there any criteria that has to be met, any boundaries, or is it just left to the two parties to figure it out? If so, I'm not sure how that helps.

Mr. Tromp: Yes. It's a very advisable measure, this November 2006 idea by the Information Commissioner, this consent order and expedited inquiry process. I believe it works that the applicant and the government body agree to a 30-day time limit to complete it, and then I believe another 30 days, and they both sign a consent order that they agree to that and fax it to the commissioner's office. Then if that deadline is missed, it's considered a serious deemed refusal. It helps a great deal to avoid conflict and litigation over time limits. This was arrived at in consultation with the commissioner and the government. They seemed to agree that it was a good idea. On the commissioner's website there's more detail about precisely how it works. It's certainly well worth studying and applying. I believe it works quite well.

Mr. Olson: In the first instance, though, it's 30 days? Is that kind of mandated, or is that left to the agreement of the parties?

Mr. Tromp: Well, 30 days is first in the law, but then after that, if I recall, it's another 30 days, and if both parties agree to that, then that's what it will be. There would be no more appeals or disagreements at that point. It seems to work well. The commissioner's office would be much better able to explain than I would, and I'm sure they'd like to.

Mr. Olson: Thank you.

The Chair: Thank you, Mr. Olson.

Mr. Tromp, thank you very much for your presentation and your time in responding to some of the questions today.

Mr. Tromp: Thank you for listening.

The Chair: You're very welcome.
Committee, we'll now move on to our next presentation of the afternoon, and joining us, again on teleconference, is Mr. David Haddad.
Mr. Haddad, before you begin your presentation, we're going to do what we did with the rest: have you introduce yourself for the record with your full name and responsibility, and the members of our committee would like to introduce themselves to you as well.

Mr. Haddad: Okay. Good afternoon. I'm Mr. David Haddad. I'm a private citizen, making a submission on my behalf concerning the Workers' Compensation Board.

The Chair: Okay. Now we'll start with the infamous Ms Blakeman.

Ms Blakeman: Thank you so much, and welcome, Mr. Haddad. My name is Laurie Blakeman. I'm privileged to be the MLA for the fabulous constituency of Edmonton-Centre.

Ms Notley: Good afternoon. My name is Rachel Notley, and I'm the MLA for Edmonton-Strathcona.

Mr. Vandermeer: Good afternoon. Tony Vandermeer, MLA for Edmonton-Beverly-Clareview.

Mr. Groeneveld: George Groeneveld, MLA, Highwood.

Mr. Lindsay: Good afternoon. Fred Lindsay, MLA, Stony Plain.

Mr. Elniski: Doug Elniski, MLA, Edmonton-Calder.

Ms Pastoor: Bridget Pastoor, MLA, Lethbridge-East and deputy chair.

The Chair: Barry McFarland, MLA for Little Bow and chair of the committee.

Mrs. Sawchuk: Karen Sawchuk, committee clerk.

Mr. Quest: Good afternoon. Dave Quest, MLA, Strathcona.

Mr. Olson: Hi. Verlyn Olson, MLA, Wetaskiwin-Camrose.

Dr. Sherman: Hello. Raj Sherman, Edmonton-Meadowlark.

Dr. Massolin: Good afternoon. Philip Massolin, committee research co-ordinator and table officer, Legislative Assembly Office.

Ms LeBlanc: Stephanie LeBlanc, legal research officer with the Legislative Assembly Office.

Ms Lynas: Hilary Lynas, director of access and privacy with Service Alberta.

Ms Mun: Marylin Mun, assistant commissioner with the office of the Information and Privacy Commissioner.

The Chair: Very good.
Mr. Haddad, we also have somebody . . .

Mrs. Forsyth: Hi, David. I'm Heather Forsyth, Calgary-Fish Creek.

The Chair: Thanks, Heather. I didn't forget you. I was just going to introduce you; that's all.

Mrs. Forsyth: Oh, right. Out of 6 you've scored 1 so far.

The Chair: I'm trying to catch up, Heather.

Mr. Haddad, you've got 15 minutes for your presentation. As you can tell, there is one of our committee colleagues who is also on teleconference, listening in, and who has the opportunity to ask questions along with the rest of us. After you're finished your 15 minutes, which we're timing as of now, we'll open the floor to questions from the committee. Please proceed.

Mr. David Haddad

Mr. Haddad: Okay. Well, I've just read my submission, and it's fairly clear what it is all about. It concerns the Workers' Compensation Board of Alberta, and it's not an uncommon complaint, I don't think. There appear to be a number of people in my position.

I did have an injury at work. It was a Workers' Compensation Board claim, the first one I ever had. I worked for Canada Post. During the administration of the Workers' Compensation Board claim they collected and released numerous documents, personal information, mostly medical, related to the injury.

One of the issues is that there's really no requirement for the Workers' Compensation Board to diagnose these injuries properly before they release the information. They appear to make decisions and collect information without doing a proper diagnosis. In my case they refused to do an MRI and such. I believe their purpose was that they like to put workers back to work as soon as possible, which is fine, but they need to diagnose the injury, obviously, before they do this.

In my case all of this information was given to Canada Post, and the issue here was determining fitness to work. Canada Post, supposedly, was supposed to be collecting their own, but they weren't. They were using the Workers' Compensation Board's files to determine employee relations. Anyway, it ended up that I had to pay for my own MRI because the Workers' Compensation Board refused my doctor's request and the physiotherapist's request for the MRI. The injury was – well, I knew it because I had the injury – much more serious than the Workers' Compensation Board was making out.

Anyway, after the MRI was done, the doctor put me off work for three months, and the Workers' Compensation Board did nothing with this information that they got from my doctor and the MRI. As a result I was terminated from my employment at Canada Post. The reason for it was the WCB claim documents that were released to them. They cited them in the termination as well.

The WCB continued to administer the claim, and what was started with the employer was an appeal of my termination. This was approximately two years later, at which time they used numerous WCB documents as evidence as well in my termination arbitration, which is contrary to the Workers' Compensation Act. At that time I called the director of legal services, Mr. William Ostapek, who was supposed to be in control of these documents, and I was told of a grey area for these documents as to what is actually part of the claim. They weren't subject to the privacy protections within the Workers' Compensation Act, because there are some privacy protections concerning doctors' opinions and files that they produce.

1:25

Now, there's been a continuous battle since then. I've been to the Attorney General, the dedicated prosecutor for the WCB, and the WCB itself. A Calgary police detective as well started an investigation. They refused to enforce the privacy protections within the Workers' Compensation Act.

I've been to the federal Privacy Commissioner. He did quite an extensive investigation, but of course he has no jurisdiction with regard to the Alberta WCB. He does with Canada Post. Apparently, there was nothing he could do about the use of these documents. I'm going to say at this point that these documents that they did use as evidence and were used to terminate were returned at an Appeals Commission hearing, and that was four years after the injury. Still there was nothing I could do about it.

You know, I've always worked. I had a job at Canada Post, and the first injury I got, I lost my employment. I've been unable to hold employment. This seems to be very common in Alberta with employers: the WCB doesn't compel them to keep injured workers on the job.

I don't know what else I could say about this. I mean, it's a very extensive submission I put in. What I really would like to ask is that the privacy protections within the Workers' Compensation Act be put into FOIP, the Privacy Commissioner's office, to administer and enforce because there's a conflict of interest between the Workers' Compensation Board and privacy protections. It's really not in their interest to prosecute employers. If it was separated from the Workers' Compensation Act and WCB legal services, I believe these protections would be enforced. You know, I did talk to the Attorney General; I talked to the dedicated prosecutor. They all say that it's the decision of the Workers' Compensation Board director of legal services. So virtually nothing has been done to enforce the privacy protections.

I see that there is a representative from the Privacy Commissioner's office there. I have asked that they be given the jurisdiction because under FOIP, as a public body, there really isn't a lot that can be done when these things happen. For the numerous people that I've been to – I've filed complaints with just about everybody – it's always a jurisdiction issue. Because I was at a federal employer and WCB is provincial, there are always jurisdiction issues. This is what I've run into right from the beginning.

That's about it, that I can say. I don't think I'm going to need the whole 15 minutes for my explanation, but I understand you're going to ask questions.

The Chair: Thank you, Mr. Haddad. We'll just take a moment here and see if there are some questions that are forthcoming after your presentation.

Mr. Haddad: Okay.

The Chair: I'll start with Heather, just in case she wanted to ask anything.

Mrs. Forsyth: Gee, Mr. Chair. Thank you.

David, at the beginning of your submission you mentioned that there was personal information that was released irrelevant to the case.

Mr. Haddad: Irrelevant?

Mrs. Forsyth: Right. You said that someone released personal information that was irrelevant to your WCB claim. Am I correct or not?

Mr. Haddad: I don't think so.

Mrs. Forsyth: Oh. Okay.

Mr. Haddad: I'm actually looking at it right here. No, I would say it was relevant.

Mrs. Forsyth: It was relevant or irrelevant?

Mr. Haddad: It was relevant, but I would say it depends on who is determining fitness to work. The WCB claims that they do not determine fitness to work for the employer. They continually say that whereas the attorney for Canada Post said that they do. I have a letter stating that to the union. So an issue here is: who does determine fitness to work for the employer? No, I think it was relevant, all of it.

Mrs. Forsyth: May I go on, Barry, or do you have other questioners?

The Chair: No, we've got others.

Mrs. Forsyth: That's okay. Go ahead. It was me who brought up the one question, so please let the other committee members ask.

The Chair: I'm just a little hesitant, Heather, because it's not really a supergood connection that we're hearing, so please ask your other question.

Mrs. Forsyth: My second question or my first one?

The Chair: Your second.

Mrs. Forsyth: Okay. David, you mentioned the fact that even though your doctor and your physiotherapist recommended that you get an MRI, it was refused.

Mr. Haddad: That's correct.

Mrs. Forsyth: Who was it refused by? WCB?

Mr. Haddad: It was the WCB case manager. There were continued requests by both of those people, and it was a six-month wait for an MRI. I actually paid for it myself eventually.

Mrs. Forsyth: But your doctor and your physiotherapist said that you should have an MRI, and if I understand, it was WCB that refused an MRI?

Mr. Haddad: Yes, that's correct.

Mrs. Forsyth: Okay. Thank you.
Thanks, Barry.

The Chair: You're welcome.

Ms Pastoor: Thank you, Mr. Haddad. One of the things that was mentioned was that you thought that perhaps a privacy advocate could perform to assist injured workers during the WCB claims process. I wonder if you could explain exactly what you had in mind when you spoke about that. Then I guess the other question would be: had you gone to an MLA or had you gone to the privacy office in the Workers' Compensation Board, and did anybody assist you?

Mr. Haddad: What was the first part of the question again? Oh, the advocate, yes.

You see, this was my first Workers' Compensation Board claim, and I knew absolutely nothing about the process. If you had somebody that would help to guide you and tell you what's going on, I think it would be much more advantageous to my employment. Like, if I knew that WCB was giving all this information out to the employer – they were copying it to the employer, and I did know it by the letter that was sent. But there needs to be somebody who can assist and say, "Well, your employer is getting this; your employer is getting that" and assist with the Workers' Compensation Board case manager because I just couldn't handle it myself. I didn't know, really, what was going on.

Ms Pastoor: Well, I guess that was what my follow-up was. Had you approached any MLAs to help you or if you'd gone to the privacy office of the Workers' Compensation Board and what, in fact, they had said about releasing your personal health information to your employer.

Mr. Haddad: I did go to David Swann, and I've copied some letters to the NDP leader, I believe. I forget his name. But, yes, I have gone. When the decision on modified duties was overturned at the Appeals Commission in 2005, they had 30 days to comply with the decision, but they didn't; it took three months. My MLA was the only one that got them to comply with it, but it really had nothing to do with my termination.

I can't remember your third question.

Ms Pastoor: If you'd gone to the privacy office of the Workers' Comp.

Mr. Haddad: I have written numerous letters. There's got to be at least a dozen concerning the information that's in there and why they distributed it. A lot of it was wrong information such as: I worked for Canada Post for 12 years, and they took it down to 10 years. There are issues like this. I've been to the Privacy Commissioner's office, who is looking at it at present, but I don't know what's going to be done.

Ms Pastoor: Thank you.

The Chair: Thanks, Ms Pastoor.
Mr. Lindsay, please.

Mr. Lindsay: Thank you, Chair. David, thank you for your presentation. It appeared, listening to your presentation, that the majority of your concerns would be covered under the Workers' Compensation Board legislation. However, it's my understanding – and correct me if I'm wrong – that you had a request that the freedom of information guidelines under WCB legislation should be removed and put under FOIPPA. Is that correct?

Mr. Haddad: That is correct, yes, because there's conflict of interest there.

Mr. Lindsay: Okay. Thank you.

The Chair: Rachel Notley, please.

Ms Notley: Thank you. Well, just following up on that line of questioning, actually, I guess I'm trying to get to the linkage between your submission and the FOIP legislation and any potential

changes. Notwithstanding my sympathy for the experience you've had with the WCB, I just want to think about how this impacts the legislation.

I'm just trying to clarify, and maybe our representative here from the office of the Privacy Commissioner can assist in some respect as well. Does the freedom of information act not at this point cover, you know, the actions of the Workers' Compensation Board such that if you had a complaint with the Workers' Compensation Board's breach of your privacy, you would not have the ability to go to the Privacy Commissioner and file that complaint and have them administer that?

1:35

Mr. Haddad: I have gone to the Privacy Commissioner, and I've tried to stick to the issues that they do have jurisdiction over, but there is no specific legislation in FOIP to deal with specific issues within the WCB. I don't know how to explain it, but it is quite clear in the WCB act, you know, how this information can be used. It's not to be used as evidence in any legal proceeding, and doctors' opinions aren't to be distributed, used as such, as it was on my case. Dealing with FOIP, it doesn't clearly define this. I've had trouble with this.

Ms Notley: I guess my question is that I understand what you're saying, and I do understand your concern about the way in which your information was used by your employer, and it's certainly arguable on the face of it that the employer didn't use it as they should have. But it seems to me that, actually, the legislation, FOIP and PIPA, also applies to that, so the Privacy Commissioner would actually have jurisdiction to deal with this.

I just want to make sure. I mean, you raise an important point; don't get me wrong. I understand. Workers' Compensation Board has tremendous access to private information, and you absolutely are correct – or I agree, anyway – that you cannot rely on them to police themselves in terms of their use of your information. But I'm just trying to determine the particulars of why it is that you can't rely on the Privacy Commissioner to police that activity. It's not clear to me that you can't.

Mr. Haddad: Okay. The Privacy Commissioner's office did a preliminary investigation, and in their decision they said that it was basically mistakes. As far as the use of the information, they cannot go to WCB legal services or the Attorney General's office and ask them to enforce the WCA, and it's pretty much under the WCA and not FOIP or PIPEDA or PIPA. I believe PIPA is federal – is it? – because I have made a complaint under that to the federal Privacy Commissioner.

It is a very complex issue, and right now I don't know how to explain it, but it seems to be that the WCA has complete control over the release of these documents and not FOIP.

Ms Notley: Well, thank you. I mean, I appreciate you raising the issue, and it's an important one. I think we'll have to get a bit more information about how these two interact with each other because it's an important issue.

Mr. Haddad: I wish I could explain it better, but I can't at this time, I guess.

The Chair: Okay. Mr. Haddad, I just have one comment. I've been looking at your submission. I just wanted to get a clarification from you. You indicated that you actually got the MRI done at your own expense.

Mr. Haddad: Yes.

The Chair: Then it was turned back in to the WCB.

Mr. Haddad: Yes.

The Chair: Was that adjudication by them then appealed by you?

Mr. Haddad: First it was given verbally to a case manager, and she pretty much did nothing about it, so I mailed it to her. Then it was put into the case file the day after I was terminated. What was the question again?

The Chair: Well, I wanted to know if once that MRI had been given to WCB, an adjudication was made that you subsequently appealed.

Mr. Haddad: Yes, there was. I went to the decision review body, and they upheld the case manager's decision. The case manager said that the MRI that I gave her would be helpful in future decisions, not the actual decisions they made, because I don't believe they were going to admit wrongdoing. So it was put into the case file at that time, after I was terminated. WCB did another one about a year later, when they determined I should be fit to work at some kind of a job, and I did appeal that to the CSRC. They upheld the case manager's decision. I don't believe they even looked at the MRI. Supposedly it wasn't an issue because I said this was diagnosed clinically without the use of the MRI, but the appeal was overturned in 2005 by the Appeals Commission.

The Chair: Is this a back injury?

Mr. Haddad: Yes, it is.

The Chair: Mr. Haddad, I want to thank you on behalf of the committee for your presentation. I don't see any other questions coming up at this point in time, but we do appreciate the time that you've taken to answer the questions and to make your presentation to us.

Mr. Haddad: Well, I thank you for listening. Thanks very much.

The Chair: You're welcome.

Mr. Haddad: Bye-bye.

The Chair: Bye, now.

Committee members, we're at a point here where we may have a couple of minutes, and I wondered if you'd be agreeable to trying to move on with some of the other business that we delayed earlier on before we have our break – it would speed up the end of the day – if that's okay with Dr. Massolin and everyone else.

Dr. Massolin: That would be fine with us, Mr. Chair.

The Chair: Very good. Would you please carry on?

Dr. Massolin: I would just like to call the committee's attention to research documents that we prepared for this committee meeting that were generated as a result of requests from the last meeting. The first of these documents is the document that has to do with budget and staffing information, and I would just ask the committee clerk to pass the updated version of this document out to the committee members right now. This document that will be passed out has

updated information, so I would urge committee members just to refer to this document and discard the earlier document if they could. You can identify this document because it's indicated on the front cover page that it's updated August 31, 2010.

Mrs. Forsyth: Mr. Chair, if I may.

The Chair: Yes.

Mrs. Forsyth: It makes it very difficult if you're passing out updated documents when we're calling in on the phone. If I may, in the future if we're going to be tabling updated documents, if we could at least have it a day earlier.

The Chair: It was posted on Tuesday, Heather.

Mrs. Forsyth: Tell me that again, Barry. Sorry; you're breaking up.

The Chair: It was posted on the website on Tuesday.

Mrs. Forsyth: Okay. Thank you.

Dr. Massolin: Yes. Thank you, Mr. Chair. I neglected to mention that the updated version is also posted on the internal website, so it's accessible there.

I just want to briefly go through this document to indicate what is going on here. As I said, this is a request from the committee from the last meeting. The document itself, unfortunately, does not contain information on budget and staffing for government ministries that are responsible for the administration of freedom of information legislation. The reason for that is that in our research we were unable to find any jurisdictions, ministries that separated out this type of information, the staffing and budget information for individuals and staff full-time equivalents, I guess, that are responsible solely for this type of legislation. So, unfortunately, this document cannot provide that information.

What we did instead was to provide this type of information – staffing information, budget information – for the office of the Information and Privacy Commissioner of Alberta and the equivalent offices for select jurisdictions across the country. We've got Alberta, of course. We've also got information here in this document from British Columbia, Saskatchewan, Ontario, and finally Quebec and Newfoundland and Labrador.

1:45

Now, there's another caveat I must mention. I hate to be sitting here and telling you what this document doesn't include, but I have to tell you that, unfortunately, I believe it's only the Alberta office of the Information and Privacy Commissioner that actually separates out information in terms of budget and staffing as to, you know, who in the staff actually works on FOIP cases or the equivalent. The other jurisdictions, unfortunately, don't separate that information out, so I want to caution committee members that the chart that starts on page 2 is not an apples-to-apples comparison. You can see, for instance, that the Alberta OIPC has, you know, the total number of case files opened, the total number of case files closed, FOIP cases opened, and then FOIP cases closed. You look at British Columbia, and the numbers are a lot higher there. Well, that's because British Columbia is dealing with a different type of caseload than is Alberta. Also, the same could be said for the budget details in terms of the monetary figures there as well.

I think the rest of the information is pretty self-explanatory, and I will of course be available to answer questions if there are any, Mr. Chair. Thank you.

The Chair: Questions for Philip?

You just made one comment, Philip, that B.C. wouldn't be handling the same type of caseload as Alberta. Can you expound on that?

Dr. Massolin: Well, what I'm saying, Mr. Chair, is that the numbers that are represented here are not reflective of the caseload that pertains specifically to freedom of information and protection of privacy legislation but, rather, the total caseload of this office, which deals with other legislation as well. I stand to be corrected on this, but I believe Alberta's OIPC is the only office, at least among the compared jurisdictions, that actually separates out this information.

The Chair: The thing that jumped out at me was that I think if I added up my numbers right, there were something like 18 people in the B.C. thing with a budget of $3.6 million and eight or so in Alberta's with a budget of $5.5 million and virtually half the files.

Dr. Massolin: Well, perhaps Ms Mun would like to jump in here, but my impression is that, again, that's not a one-to-one comparison there because of the different responsibilities and mandates of the offices.

The Chair: That's why I was trying to figure out what that difference would be.

Dr. Massolin: I don't know if Ms Mun would like to jump in on that one. I mean, as it says here in the note for British Columbia, "staff are not primarily responsible for cases under certain pieces of legislation." So it's just mixed and matched a little bit differently here.

The Chair: No, that's fine.

Dr. Massolin: Sure. It's a valid point.

The Chair: When I first read it without that explanation, I thought: hmm, things are different. I thought it was apples to apples.

Dr. Massolin: Right.

The Chair: Let's move on.

Stephanie.

Ms LeBlanc: Thank you, Mr. Chair. I'm briefly going to go over the other two documents that were posted on the committee's website. I'm looking at the cross-jurisdictional comparison as well as the research briefing. Both of these documents are dated August 25. The cross-jurisdictional comparison considers five issues that were raised by committee members.

The first question asked was to what extent the legislation in other jurisdictions applies to third parties that provide services to the public as a result of receiving public funding or by being the recipient of delegated legislative authority. In the compared jurisdictions the legislation does not automatically provide that an organization becomes a public body under the legislation for either of these reasons. However, British Columbia's legislation does make certain provisions of the act applicable to persons or organizations contracted to perform a service for the public body.

The second issue raised was whether public bodies in other jurisdictions are required to publish information holdings. In five of the seven compared jurisdictions, public bodies or the minister responsible for the legislation are required to publish a directory of

personal information banks, which would be directories that contain personal information. In four of the jurisdictions a document has to be published that contains general information regarding the types of documents that are used that are in the possession of public bodies.

The third question asked for information regarding the timelines for access requests and inquiries, and the charts on pages 13 and 16 of the document show these timelines. One clarification that should be made with respect to these charts is that British Columbia's legislation defines "day" as excluding weekends and holidays, so even though there is a 30-day period and a 90-day period, the timelines in B.C. would be longer than a jurisdiction with a similar timeline.

The fourth question asked for a comparison of the exceptions to disclosure in other Canadian jurisdictions. The chart on pages 17 and 18 has a short description of the exception in the far left column and then an indication as to whether a particular jurisdiction has the exception or not.

Finally, section 3.7 of the report contains a comparison of the fees for access to information across Canada, which was provided to our research group by Service Alberta.

The next document is the research briefing, also dated August 25. Research staff were directed to provide an analysis of issues raised that suggest that clarification of provisions of the FOIP Act is required. We looked at 12 different issues, and those were taken from the submissions. Those 12 issues are listed in the table of contents, which is just on the flip side of the cover page. Since we're short on time, I won't address these issues in detail, but I'd be prepared to answer any questions from committee members.

Thank you.

The Chair: Thanks, Stephanie.

Any questions from any of the committee members, starting with Heather?

Mrs. Forsyth: No. I'm fine thanks, Chair.

The Chair: Okay.

Thanks for all the work you guys have done in putting this together. I'm sure we'll have some questions as we go forward on some of the recommendations. This is what we'll be able to use to compare when we're making a recommendation, then, Philip?

Dr. Massolin: Yes. Thank you, Mr. Chair. I am glad you mentioned that because I was going to mention to the committee as well that, of course, these documents may remain pertinent as the committee begins its deliberations a little bit later on.

Thank you.

The Chair: Good. Seeing no more questions, then what we're going to do is take a quick break of eight minutes, a relief break if you will, and then we'll be back for our final two submissions.

[The committee adjourned from 1:52 p.m. to 2:01 p.m.]

The Chair: Welcome back, ladies and gentlemen. It is time for our afternoon presenters.

I'd like to welcome our next speaker, whom we've asked as an expert to come in, Mr. Alec Campbell. At the last meeting there was interest expressed that we find a private-sector expert to appear before the committee to discuss the role of information technology as it relates to the FOIP legislation.

Alec Campbell is the president and principal consultant of Excela Associates Inc. He's been involved in the administration of freedom of information and privacy legislation since 1993. Mr. Campbell is here today as an independent consultant to discuss these matters from his perspective. He has and continues to hold contracts with the government to provide training and expertise. It should be noted that his appearance here today does not necessarily represent the views of Service Alberta or the government of Alberta.

With that, Mr. Campbell, I want to again thank you for making your presentation. Just for the record if you would give your full name and your title. You have 30 minutes to make your presentation because we've invited you; you hadn't made a presentation to us. Then we'll open the floor to questions from the committee after we've introduced ourselves as well.

Excela Associates Inc.

Mr. A. Campbell: Thank you very much, Mr. Chair. My name is Alec Campbell. I'm president and principal consultant with Excela Associates Inc.

Mr. Chair, hon. members, thank you for inviting me to speak to you today. I hope that I can provide some information concerning the emergence of new information technologies, especially their impact on the accessibility and governance of personal information. I'll also raise some related issues that may be of relevance for your review of the FOIP Act. Whether or not they require amendments to the FOIP Act, the issues I raise are significant for the administration of FOIP compliance by public bodies in Alberta. You, of course, will decide whether amendments are appropriate for the issues I address.

Much of my work involves the interface between information technology and privacy. There are many issues associated with the impact of information technology on privacy and access to information. Generally speaking, information technology issues have a greater impact on privacy protection than they do on access to information, although I will mention a few areas in which access may be affected. Because of our time constraints today I'm going to limit my comments to four information technology issues of significance for FOIP administration: extraterritoriality, cloud computing, data consolidation, and security. I'll spend most of my time on cloud computing. Before I touch on that, though, I'll touch on extraterritoriality.

Extraterritoriality isn't just an IT issue, of course, but it is significant for decisions regarding data storage and other aspects of information processing. What we're talking about here is the application of a nation's laws beyond its boundaries.

The USA PATRIOT Act and similar national security legislation in other countries has been a topic of discussion for several years. There have been concerns that personal information about Canadians might be subject to unauthorized access by foreign security services if the information is located on foreign soil or even if it's located on Canadian soil but under the control of organizations subject to foreign laws, subsidiaries of American companies located in Canada, for example. The United States courts are known for their lack of reticence when it comes to the extraterritorial application of United States law.

In response to these concerns amendments were made to the FOIP Act and equivalent legislation in several other jurisdictions in Canada with the intention of making it more difficult for service providers to comply with extraterritorial demands for personal information that's located in Canada but under the control of the service provider. FOIP Act amendments also introduced penalties for public bodies that provided personal information in response to demands from courts without jurisdiction in Alberta.

While these concerns have merit, Canadian national security legislation is largely equivalent to such legislation in many other countries, including the United States. Also, existing treaties would often provide access to personal information about Canadians, in any event. It's therefore not entirely clear whether the extraterritorial application of foreign law significantly increases privacy risk for Albertans. In any event, in my opinion, there's little more that could be done within the FOIP Act itself.

With that, I'll move on to cloud computing, which, with the possible exception of security matters, is probably the most popular topic of discussion today concerning privacy and information technology. This is because cloud computing creates a new paradigm for the custody and control of user data, including personal information, a paradigm that shifts the nexus of control from the client to the service provider. At the same time it offers economies and operational advantages that make it hard to resist for individual and enterprise users alike.

Before I go further, we need to be clear about what we're discussing. The term "cloud computing" refers to computing services and applications in which both the application and the related data storage reside in remote locations and are accessed via Internet connections. The application is online and so are the data. Consequently, the application and data may be located anywhere in the world with an Internet connection. Both data and application are often geographically far removed from the user. This gives rise to a number of factors affecting privacy protection, some of them obvious and some not so obvious.

The first factor is legal jurisdiction. In a cloud computing environment the legal jurisdiction of the service provider is often different from the legal jurisdiction of the user. In Alberta this is almost always the case since few cloud computing services are hosted in Alberta. From a FOIP perspective this means that the service provider is not subject to FOIP or to other provincial legislation such as the HIA or PIPA even though the public user is. If a public body contracts with Google to provide its e-mail services, as some have done, both the e-mail application and the content of e-mails are hosted outside Alberta. In fact, they're hosted outside Canada.

The risk here is that the legislation of the hosting jurisdiction may not require a standard of privacy equivalent to that required by FOIP. This could diminish the level of privacy protection the public body can offer, possibly to below FOIP compliance thresholds. This makes the contractual relationship between the public body and the cloud service provider extremely important, but usually cloud service providers require the use of standard contracts drafted in their own jurisdictions. When that jurisdiction is in the United States, the privacy standards reflected in the contract are often far below the privacy standards required by FOIP. I'll speak to contractual issues a little more later on.

The larger problem is actually more mundane. It is quite simply that it's difficult to know what legal standards apply to the protection of personal information when it's located in jurisdictions outside Alberta. Canadian privacy legislation is fairly consistent, and most privacy practitioners have few concerns with personal information being located in other Canadian jurisdictions. Once personal information leaves Canada, though, it may be subject to quite different privacy standards or, indeed, to none at all.

It's therefore incumbent on any public body that considers storing personal information outside Alberta, especially outside Canada, to know what privacy and security standards will apply to that information. That's often harder than it sounds. It's also incumbent on any such body to contractually bind service providers to a standard of privacy equivalent to that provided in Alberta. For reasons I've already mentioned, that's also more difficult than it may sound, and I'll speak to it a little more later.

2:10

The second factor associated with cloud computing is what I call geographic dispersion. It's related to the previous factor, but it has its own implications. By geographic dispersion I mean that in addition to data being geographically removed from the user, the data may be geographically dispersed among various physical locations, indeed various countries in some cases. Cloud computing service providers are able to locate their data, any user data, anywhere they wish. They're unconstrained by the geographic location of the user, and indeed they are unconstrained by their own geographic location as well. Furthermore, though, one user's data need not be located in just one place. Even a single file can be split among different servers in different physical locations as a result of load-balancing algorithms and other factors.

One example, a personal example here. A couple of years ago I was looking at online backup solutions for my company. I found one that was at the right price point and seemed to have the features I required. I was almost ready to subscribe to it until I found out that the service used servers in several different countries, 16 of them, to be exact, and that any one user's data could be spread among any or all of those servers. That actually could be an advantage from a security point of view, at least from an antihacking point of view, because it would make unauthorized access more difficult. You'd have to access all of the servers to get access to any of the single files that were spread across them.

But the problem was that it also made it impossible for me to tell my clients exactly where their data was. I had no control over the legislation affecting my backup data since new servers were being added in new jurisdictions all the time and others were being shut down for various reasons. As a result, I had to look elsewhere for my backup solution. I couldn't provide adequate notice to my clients related to the location of their personal information.

In addition to complicating issues of legal jurisdiction, the geographic dispersion of data can potentially create problems for some FOIP access requests. Under some circumstances – and I'm not suggesting that this would occur that often, but it is a possibility – it may be difficult for public bodies to thoroughly search their records if those records are housed in the cloud, especially if such searches require the use of search tools not provided by the cloud service provider. Cloud service providers often have proprietary software which is an integral part of their services, and because your data are located on their servers, it sometimes is accessible to the end user only through the software provided by the service provider. If you need to search the data in a way that isn't supported by that search tool, by the tools that the service provider provides, that could be a problem in some circumstances for general access requests.

There's another issue, too, and that is that if data are spread among multiple servers in multiple locations, you have multiple points of failure. From a security perspective, for example, a power outage in any one of those servers could prevent access to the data. That's not unique to cloud computing, of course, but it is a factor.

That leads us into the third cloud computing factor, which is security. A couple of years ago a blogger made the following statement about cloud computing, which rings pretty true for me. He said: a well-configured cloud computing architecture is a hacker's worst nightmare; conversely, a poorly configured cloud computing architecture is a hacker's best dream. What he's getting at is that cloud computing services are not necessarily problematic from a security perspective. In many cases, in fact, they are superior to the security provided by equivalent locally hosted applications. This is because cloud service providers typically require large data centres

for large volumes of user data. Such data centres are normally better secured than computing environments in smaller organizations.

On the other hand, though, such large agglomerations of data are big targets. They are very attractive to hackers, criminal organizations, and others who may seek unauthorized access. The volume of personal information in large data centres can have considerable black market commercial value. Large data centres also tend to have relatively large numbers of technicians, increasing the risk of unauthorized access by insiders. Furthermore, privacy or security breaches often have much larger implications when they involve data centres than when they involve small, locally installed servers.

Another factor to consider is data persistence. Basically, what I mean by data persistence is the difficulty in deleting data. With cloud service providers it can be hard to get rid of your data if you want to. This is a big privacy factor with certain kinds of cloud computing services in particular such as social networking sites like Facebook, which are a form of cloud computing. Users may find it difficult or even impossible to delete their data from the servers. Even if they're successful, there's no guarantee that the data haven't been copied or replicated elsewhere on the Internet. For example, some Facebook applications maintain their own databases of Facebook user data, and those databases may not synchronize deletions with Facebook's own servers.

This isn't an issue with all cloud computing applications. It usually only applies to those that are intended to make user data available to a larger public. Corporate cloud computing environments usually include data management features that reduce or eliminate this risk for corporate data. Nevertheless, public bodies considering the use of cloud computing services must ensure that all their data can be permanently and irretrievably deleted from the service provider's servers on demand or when the services are terminated. I would consider a service provider's unwillingness or inability to provide ironclad guarantees in this regard to be a deal breaker in every case.

That leads into a little more discussion around contractual controls. All of the factors I've mentioned so far mean that when FOIP public bodies consider the use of cloud computing services, contractual matters are all important. Because of the issues raised above, it's critical that the contract between the public body and the service provider impose conditions equivalent to those imposed by FOIP on the public body. Even then there are always potential problems associated with the fact that the service provider is subject to different laws than the FOIP public body. Since a contract rarely trumps legislation, if there's a conflict between the FOIP standards reflected in the contract and the legislation in place in the service provider's jurisdiction, the legislation will usually prevail.

I noted earlier that most cloud service providers strongly prefer to use their standard contracts rather than custom contracts for individual clients. In some cases they may completely refuse to enter into custom contracts. In other cases there may be a willingness to modify certain provisions of the contract or to consider custom schedules, additional schedules to the contract, such as a privacy schedule for larger clients, but unfortunately small organizations and individual users will usually be out of luck.

This is a major consideration for public bodies considering the use of cloud computing services. Public bodies, especially government of Alberta departments, are accustomed to drafting their own contracts with service providers. When dealing with cloud computing service providers, though, they may face the same kind of situation they often face when dealing with major chartered banks; namely, that the standard service provider contract is a take-it-or-leave-it deal. They are not prepared to open those contracts. That can be a problem because the standard cloud computing service contract rarely provides sufficient provisions to ensure that the service provider meets a standard of access and privacy equivalent to that required of the public body under the FOIP Act.

How, then, do we look at mitigating some of these risks? There are a couple of possible legislative approaches to at least a partial mitigation of some of the risks that I've mentioned associated with cloud computing. First, any public body considering the use of cloud computing services involving personal information could be required to prepare a privacy impact assessment and submit it to the OIPC for review. This would be similar to the section 64 PIA requirement in the Health Information Act except that it would apply in a much more limited set of circumstances. In a moment I'll mention one other circumstance in which mandatory PIAs might also be considered.

2:20

Second, the act could be amended to explicitly require public bodies to contractually ensure that computing services and data storage located outside of Alberta comply with the public body's obligations under the FOIP Act. This obligation exists today, but it's not as explicit as it could be, and it's unclear whether all public bodies realize the full extent of their obligations in a cloud computing environment. However, because of the reticence of service providers to enter into custom contracts, this could reduce the number of service providers available to public bodies.

Having said that, local legislation on where the data are stored, as I've noted earlier, will usually override any contract between the service provider and the public body. There's only so much that public bodies can do contractually where there's a potential for conflict with legislation. In many cases, though, the conflict isn't with legislation; it's with the service provider's own policies and procedures, in which case contractual terms can be of great assistance.

Another issue associated with information technology is data consolidation. This is something I'd like to mention specifically in relation to data consolidation and data sharing initiatives within the government of Alberta. As personal information proliferates across government and as pressures to more efficiently process that information increase, there's some pressure to consolidate stores of personal information and use those consolidated stores to service projects and programs in various departments of government.

While efficient data processing is an admiral goal, great care must be taken to avoid the perception that the government of Alberta is or should be a single public body for data sharing purposes. The FOIP Act was drafted in such a way that departments of government were deliberately defined as separate public bodies. The intent of the drafters was to ensure that the collection, use, and disclosure of personal information by government was subject to strict controls, including controls on the exchange of personal information between departments.

The uncontrolled proliferation of personal information across government would seriously compromise the personal privacy of Albertans. It's incumbent upon the government to ensure that such proliferation doesn't occur. Clear standards are required to govern government of Alberta data sharing initiatives that involve the regular exchange of personal information. Whether this occurs through binding government policy or through legislation is not particularly important in my mind, but it must occur.

Given the potential for widespread proliferation of identifiable personal information across government departments, the privacy risks and implications of data sharing initiatives should be subject to rigorous formal assessment. In my opinion, it would be worthwhile to consider making privacy impact assessments mandatory for

projects or systems involving the regular exchange of identifiable personal information between more than one public body. To be effective, such assessments would have to be subject to review by the commissioner. Although large-scale data sharing initiatives often produce privacy impact assessments for review by the commissioner today, making such assessments mandatory would ensure that they're always undertaken, and that's not the case today.

The last issue I'll mention is security. Security is and always will be a critical issue for FOIP administrators dealing with information technology. I've already mentioned some security factors associated with the cloud computing issue. There are many other security risks that are not uncommon among public bodies, including inadequate access controls, high-risk data storage practices such as the failure to encrypt laptop hard drives, excessive reliance on service providers for security planning, inadequate disaster recovery plans, and so forth. The Auditor General has raised a number of these issues in reports over the last several years. There's no time today to delve into them in any detail, but I'd be remiss if I didn't mention them as significant risk areas for FOIP compliance. In my experience, many of these risks affect smaller public bodies more than large ones, but large public bodies are certainly not immune.

Section 38 of the FOIP Act currently requires that public bodies make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction. This provision imposes a general security obligation, but it provides no direction on how to meet that obligation. I'm not suggesting that the FOIP Act should be prescriptive in security matters. Given the rapid evolution of information technology and the security measures it requires, a prescriptive approach is clearly inappropriate. However, there may be room for some elaboration without becoming prescriptive per se. There's reason to consider this. Especially in smaller public bodies there definitely remains a gap in understanding regarding IT security requirements.

For example, the act could require that in addition to its current language there be physical, administrative, and technical measures implemented to protect the confidentiality, integrity, and accessibility of personal information. This would ensure that public bodies consider all the cells of a security taxonomy, which comprises physical, administrative, and technical measures on one axis and confidentiality, integrity, and accessibility on the other axis. Both such axes reflect common and well-understood categories of security measures. Such wording would help to ensure that public bodies cover the security bases, as it were, without restricting them to any specific set of security measures.

One other consideration is of course the issue of breach notification. As you're well aware, Alberta was the first province to require breach notification under the Personal Information Protection Act. I won't discuss this at any length. I think it suffices to say that if private-sector organizations have obligations in this area, it can be argued pretty convincingly that public-sector organizations should have the same obligations.

In concluding, just by way of summary, I've mentioned three areas in which amendments to the FOIP Act might be beneficial to help address information technology issues. These are mandatory privacy impact assessments under certain circumstances, expanded language concerning security measures, and a breach notification requirement similar to the one in PIPA. I'm not suggesting that the act is severely flawed in any of these areas, but there's always room for improvement.

I'll conclude on that note. I'd be happy to respond to any questions you may have. Thanks again for the opportunity to speak.

The Chair: Thank you very much.

Mr. A. Campbell: Thank you.

The Chair: Mr. Campbell, it looks like you must have timed yourself on the presentation.

Mr. A. Campbell: Yeah, I did, actually.

The Chair: It's my pleasure now to open the floor up to questions from our committee members. I know there were some who'd asked about certain issues and wanted to . . .

Mrs. Forsyth: Mr. Chair, I can't even hear you.

The Chair: I'm sorry. I moved the mike. I was just telling Mr. Campbell that I knew that some of the committee members had asked for an expert in here to answer some of the questions that they had, so now is the opportunity for our committee to ask those questions.

Mrs. Forsyth: I have a question for him if you could put me on the list, please.

The Chair: You can start right off.

Mrs. Forsyth: Thank you, Mr. Chair. Thank you, Mr. Campbell. I enjoyed your presentation. I just want to maybe get some clarification on this cloud computing that you were talking about so that I understand it. What's happening now is we have a lot of businesses that are having people doing solicitation; i.e., they're calling from India, et cetera. Are you saying that if those calls are generated from India or something, their privacy legislation is different than what ours would be and we're subject to all sorts of openness in the privacy legislation in places like that?

Mr. A. Campbell: Well, in some places they may be. India has just passed privacy legislation, and I am not familiar with it at all. But that is the essential risk: that in certain locations to the extent that they're collecting or storing personal information, that information may be subject to different privacy standards than exist under FOIP in Alberta. To the extent that a public body is unable to delegate privacy protection to a service provider, that becomes an issue for the public body because it has to ensure that the standards to which it is obligated under the FOIP Act can be replicated by its service provider regardless of where they're located.

Mrs. Forsyth: If I may, Chair.

The Chair: Yes. Please go ahead.

Mrs. Forsyth: I guess I'm trying to follow through with this. For example, can my personal privacy information be sold to – say they're doing solicitation from India – someone else so that they can call me? This hearkens to, like, telemarketers, et cetera. I sometimes wonder how the heck they get your information.

2:30

Mr. A. Campbell: Well, first off, I think you're speaking more of private-sector situations than public-sector ones. Certainly, in the private sector that can happen if there aren't adequate contractual controls over the subsequent distribution or dissemination of personal information, and if there are no legislative controls in existence in the jurisdiction in which the information is being held, there is a risk, then, that your personal information might end up somewhere you wouldn't expect it to end up. To the extent that

public bodies may consider – India may be an extreme example. In most cases the cloud computing services we're talking about are located in the United States or, to a lesser extent, in Europe, but they may have servers in India, so data may still be located there as well.

Mrs. Forsyth: Thank you so much.

The Chair: Thank you.

Ms Blakeman: Well, that was an excellent presentation. I'm really glad the committee asked you to come in. It's exactly the kind of context that I was looking for to help understand. I'm really discouraged right now, actually, because I think sometimes we're fooling around with the small stuff while the big stuff just stomps us.

Okay. Cloud computing. Let me back up. The Ontario Privacy Commissioner is out campaigning right now for a new system called privacy first or something.

Mr. A. Campbell: Privacy by design.

Ms Blakeman: Thank you. Privacy by design. I was struck with that, but in light of what you're telling us, how could we take ourselves back a step and set ourselves up better to protect our citizens? Is it a matter at this point that we would just have to give up participating in certain services or certain sectors that are out there in the world right now? In other words, are we already too late in how we organize ourselves? For example, data storage. I mean, if we said, "Okay, that's it; nobody that is going to have off-Alberta-soil data storage is going to get any of our government or public body business," would we be able to function?

Mr. A. Campbell: You probably could function because cloud computing is very recent. As an effective commercial product it's probably only about five years old. Before that most data was hosted locally or at least with local service providers: Telus, that sort of thing, service farms that were located fairly nearby. I think what's different now is the emergence of large-scale cloud service providers, which can offer very substantial economies, price reductions to public bodies and other organizations. It becomes an issue of balancing cost and operational efficiencies against the standards imposed by legislation, including the FOIP Act but not exclusively the FOIP Act.

As far as what we do about it, the key is in the contract. I think that if there is anything that would assist, it would be to find ways to encourage cloud service providers to be willing to adopt some provisions that they might not otherwise adopt related to FOIP responsibilities around the protection of personal information. So in a number of cases, not dealing with cloud computing but dealing with other contractual relationships, public bodies have added privacy schedules to their contracts. Basically, they either tack on a schedule to the back of the contract or they embed provisions in the contract itself which replicate the requirements of the FOIP Act and ensure that the contract then imposes those requirements on the service provider.

Where you can do that, that's quite an effective approach. The problem arises when the service provider won't consider that kind of contractual amendment. At that point the public body has no choice but to decide whether or not it's going to absorb the risks and go ahead with the contract or not.

Ms Blakeman: But I would argue that given that the government is the only one that's in a position to form that contract or not, it is the government's responsibility to say, "Well, then we're not going to sign it if you will not sign privacy provisions or add a rider," as you say. But how much does that damage our global competitiveness as an economic body?

Mr. A. Campbell: Well, I don't know that that's always going to be the case. It's really a matter of assessing the risk associated with a particular service as applied to a particular set of personal information. The volume of information you're dealing with, its sensitivity, all kinds of factors come into play in the decision, and that's why I'm suggesting that formal, well-conducted privacy impact assessments are critical in these decisions. In some cases it may be that relatively minor amendments or even none at all are adequate. In other cases they won't be. But you need to do a thorough assessment to determine that in each case, I think. It's a due diligence exercise, basically.

Ms Blakeman: Could I get one more supplemental in? Is there a long list?

The Chair: We have quite a list.

Ms Blakeman: Oh, okay. Put me on the end, please.

The Chair: I certainly will.

Ms Notley: Mine, I guess, sort of follows to some extent on what we were just discussing. I might have missed the point here, but I also don't sort of get where the solution lies in this information that you're providing to us because even where you do negotiate the contract, you're still then subject to whatever the extraterritorial laws are.

Mr. A. Campbell: Where there is a potential conflict with legislation, yes.

Ms Notley: Right.

Mr. A. Campbell: But, you know, that's not always the case. In many cases it's just a matter of the service provider having inadequate security measures, for example. There's no conflict with legislation.

Ms Notley: Right. Okay. I thought I had heard you say that you could negotiate our standards into a contract but that if our standards didn't exist in the legislation in the country where the information resides, then our contract might be ineffective.

Mr. A. Campbell: No, I wouldn't quite put it that way. If FOIP standards are negotiated into a contract and there's a direct conflict with legislation in the jurisdiction in which the data are held, then the legislation is likely to trump the contract. That most often arises in one of two circumstances, either where there's some kind of civil litigation that demands the information that's being held or where security services demand it. That's where I was saying that may be a factor. Especially where the security services are involved, there are often other ways for them to get the information anyway. But where those two kinds of things don't arise, where it's just a matter of ensuring that the service provider provide a level of service equivalent to what the public body would want to provide, the contract can be an effective means of doing that.

Ms Notley: What are you proposing is the best mechanism in terms of the work that we're doing on this legislation to deal with these risks?

Mr. A. Campbell: I don't think there's too much that can be done in terms of the legislation itself around contracts unless you're prepared to limit the choice of cloud computing service providers for public bodies. If you're prepared to do that, you could impose requirements that explicitly subject public bodies to the obligation to ensure that their contracts reflect their FOIP obligations.

I think more realistic is a requirement either in legislation or in binding government policy that all potential contracts with cloud service providers not located in Alberta be subject to privacy impact assessments and that those privacy impact assessments be reviewed by the commissioner, as I say, similar to the requirements in the HIA. That way at least you're doing a solid risk assessment in each case.

Ms Notley: Okay.

2:40

The Chair: Thanks, Ms Notley.

Mr. Vandermeer, followed by Mr. Olson.

Mr. Vandermeer: Yeah. My questions were also along the same lines, so you pretty much answered them. I guess what we have to do as a government is just make sure that our contracts are very sound. I think you've answered that question.

Mr. Olson: Thank you very much for the information. It's been really enlightening and a little bit disturbing, too. It makes me realize how old I am because I can remember as a young lawyer studying conflict of laws, which was my least favourite subject – it has to do with, you know, what laws apply in the case of contracts and any number of other things – and I realize how much the world has changed in the last, dare I say, 35 years.

It does make me wonder about whether or not there are any international convention or treaty obligations, those types of things, that might give us a little bit of comfort. If we know that another jurisdiction has signed on to some sort of treaty obligation or convention, that would at least assist with enforcing what's there. I mean, I can counsel lots of clients on contractual issues, where even a contract with one of the parties in Saskatchewan I would say: how are you going to enforce it? It's going to be a lot more complicated enforcing it if you have to go outside of Alberta. I can only imagine how much more complicated it can get dealing with a host of other jurisdictions. It's fine to say that you've got it in a contract, but enforcing it is completely another matter. If you've got, you know, some understanding with those other jurisdictions that they will enforce the contractual obligations that have been made, at least we have something. Are you aware of anything like that?

Mr. A. Campbell: Well, unfortunately, the United States, as you probably know, has no overarching privacy or data protection regime, although there are privacy requirements embedded in certain sector-specific legislation, health care for example. The European Union, though, has a pretty solid set of data protection requirements, and personally I wouldn't be too concerned about hosting personal information in most European Union countries, although I don't profess to be an expert in their privacy legislation. The United States is more difficult.

Australia and New Zealand don't currently host cloud computing services very much, but their legislation is, you know, reasonably equivalent to ours. Same in Hong Kong.

I wish I knew more about India's new legislation because that is, clearly, a very important country for the kind of issues that we're talking about. India hosts a lot of remote computing services, but unfortunately I simply can't speak to their legislation right now.

In terms of international conventions or treaties, though, there's nothing overarching that I'm aware of.

Mr. Olson: Okay. Thank you.

The Chair: Thank you.

Dave Quest, followed by Dr. Raj Sherman.

Mr. Quest: Thank you, Mr. Chair. This has been very enlightening, for sure. You mentioned – and I'd maybe refer this to our legal people later – in section 38 "reasonable security arrangements." In your opinion that is not sufficient.

Mr. A. Campbell: Well, as I said in my presentation, it certainly places the obligation on the public body to ensure that they have adequate security in place. I think, though, it might be helpful for some public bodies, at least, to have a little more direction on what reasonable security arrangements would typically entail. That's where I'm suggesting the use of these common categories of security measures that you will frequently see in security-related documentation. If the legislation were to require that security measures include measures in each of the nine categories that would be created by that three-by-three table, we would have gone a much, much longer distance in ensuring that potential threats were adequately covered off, but we would not have gone so far as to tell public bodies what measures they had to take to cover off those risks.

Mr. Quest: If I can just have a quick supplemental, Mr. Chair. Breach notification requirement: is this common in other jurisdictions? Even if it is or isn't, who gets notified: us and/or the person?

Mr. A. Campbell: In the case of the PIPA provisions the commissioner gets notified, and then the commissioner determines whether or not notification needs to go to individuals who might be affected as well. That doesn't prevent the organization involved from directly notifying individuals, but they don't have to do that. What they have to do is report to the commissioner where they believe that a significant breach of privacy has occurred.

Other jurisdictions. I think it's about 40 of the 50 states in the U.S. that now have breach notification legislation. They don't have commissioners, so it usually requires public notice, notice to any affected individuals. In Europe there is some emerging discussion around breach notification, but I'm not aware of specific provisions. Marylin might be able to help me there, but I'm not sure. Elsewhere in Canada currently Alberta is the only jurisdiction with breach notification, but it appears that it probably will be included in future amendments to the federal legislation.

Mr. Quest: Thank you.

The Chair: Thanks, Mr. Quest.

Dr. Sherman, followed by Ms Pastoor.

Dr. Sherman: Thank you, Mr. Chair. Mr. Campbell, thank you so much for your presentation. As I sat here, I was just daydreaming that I was in a time warp. I used to be a computer geek 30 some-odd years ago on the Apple II Plus computers, where you had to learn all the languages. Never in my wildest dreams would I have thought we'd be discussing these issues today and that technology would have progressed to this point, which leads me to believe that 30 years from now my children will probably have the same concerns that I'm having today.

Just personally – I think I mentioned this before – my information was taken from a dentist's office. There was a privacy breach there. My Visa card was used all over the world in a matter of a few hours. They cancelled my Visa. I think my computer got broken into, hacked by somebody from China. Then my car got broken into two weeks ago. I think the computer hacking was worse than the car getting broken into.

Mr. A. Campbell: Probably.

Dr. Sherman: We discussed one of the most significant pieces of health care legislation recently, amendments to the Health Information Act, and health care information and data and how we use technology are going to significantly improve how we deliver health care. However, the privacy of your personal medical information and protection of that privacy are of utmost importance in the success of the health record. As legislators and as people who are responsible, who in the world does this the best? Who has the best legislation, the best policy, the best systems, and the best protection systems? How should data be stored and protected, and what are the future risks that you see?

Mr. A. Campbell: Well, in answer to your first question, in my opinion Canada has the best protection in existence right now. There are, as I said, other jurisdictions that have similar legislation, notably Australia and New Zealand, but other than that, there are significant gaps, in my personal opinion, in the legislation of virtually every other country. I think we have the most comprehensive privacy regime out there today.

In terms of your third question, I spoke for half an hour on some of the issues and risks that we see, and I think we just have to continue to ensure that due diligence is undertaken when we consider new approaches to the management of personal information, whether it's for health care or for any other purpose.

I'm sorry; I've forgotten your second question.

2:50

Dr. Sherman: How should the data be stored and protected? Who actually physically protects health data the best right now?

Mr. A. Campbell: I think most of the major electronic health record systems are fairly effective in terms of how they protect the data in the data store, so their actual databases are pretty well protected. That's not typically where the risk most often lies. The risk lies with the users and ensuring that the right users have access to the right data but only to the right data and that they know what their responsibilities are in terms of protecting that data.

That said, there are some things that could be done better. In my opinion, data encryption is not widespread enough today. I think there's quite a bit that could be done to improve access control through encrypted data, particularly for mobile devices. I know the commissioner has said frequently that the minimum acceptable security measure for portable data is encryption. There are still many public bodies who are not using encryption for portable data.

Dr. Sherman: Thank you.

The Chair: Thanks, Dr. Sherman.

Ms Pastoor: Thank you very much, Mr. Campbell, for that presentation. The language that you used probably went over my head because I'm not even close to being a computer geek, but the message and the concept, certainly, I think we've been aware of for many years. I guess the point is that if an 11-year-old can hack into the Pentagon – hello? – what chance do the rest of us have?

My concern, like Dr. Sherman's, is also on the health care records. It, quite frankly, scares the hell out of me when I think of the use or misuse that people could have when they get their hands on that kind of information. I'd like a comment on if you think it would be helpful or if it would control if we had a harmonization of the privacy legislation between Alberta's PIPA, the federal Personal Information Protection and Electronic Documents Act, and also Alberta's Health Information Act, if there was some sort of – I don't know – a collation between all of these, if there was that harmonization, if that would help at all in terms of, particularly, protecting health. A lot of these do overlap. Some of them sort of say the same things. It's public-private because, clearly, we are going to have to worry about private health records. As more and more private deliverers come onside, they are going to have a tremendous amount of information that I believe should be protected by a public body.

Mr. A. Campbell: Well, we could easily use up the rest of the day and more on those issues, and to tell you the truth, I didn't really come prepared to talk about HIA issues very much. The only thing I would say in response is that the different pieces of legislation are geared to the protection of privacy in different sets of circumstances. For example, in the private sector privacy is all about consent. It's all about you saying: what's going to happen with my data? If you don't like what a given company does with it, you can usually go to another one. In the public sector that's not the case. In the public sector it's all about legislative authority because often the data collection is mandatory in some sense of the word, and even if it isn't mandatory, you know, there's only one place you can go for the particular service.

In health care it's different yet because in health care there's a strong requirement for the free flow of personal information between health care providers to ensure that the services provided are the best possible. In each of those sets of circumstances you tend to arrive at slightly different kinds of privacy rules, and I'm not sure that it would be possible or even, really, desirable to attempt a complete harmonization of those rules.

I think, though, that the principles behind the privacy legislation across Canada, including all three of our privacy acts – FOIP, PIPA, and HIA – are pretty consistent. If you look at what are known as the fair information practices, which came out of an OECD document on data protection in 1980, all of our legislation is vested in those principles to some degree, so at that level there is a certain degree of harmony.

Ms Pastoor: Thank you.

The Chair: Thanks, Ms Pastoor.

Now Mr. Vandermeer and, if we have time, Ms Blakeman.

Mr. Vandermeer: Thank you. We always talk about value-added here in Alberta, that we don't want to just ship our raw bitumen to the States and then refine it there. What if we were to say: if you want to store Albertans' data, you have to store it here in Alberta? Do we have companies that have the capacity to do that here?

Mr. A. Campbell: The answer to the second question is yes. In terms of data storage certainly there is that capacity in Alberta. When we're dealing with cloud computing, though, in particular, we're also talking about the application. The applications that are of greatest interest to many enterprises today are not hosted in Alberta, so there's some trade-off there. Certainly, organizations

like Telus, for example, have large, very secure server farms, and those are located in Alberta. There was government policy at one point that restricted the location of data for the government of Alberta, government of Alberta owned data as it were, to either Alberta or somewhere else in Canada, that discouraged the location of data outside of the country, certainly, and to a lesser extent outside of the province. While I'm not sure if that policy itself is still active, that is still the position of many government departments. They will avoid locating data outside of Canada where they can.

Mr. Vandermeer: Thanks.

The Chair: Thank you, Mr. Vandermeer.

That hour went by extremely quickly. On behalf of our committee I'll make one observation. This is the least informed person when it comes to technology compared to my colleagues here. When I watch that blond gal on *Criminal Minds* who can hack in and get all kinds of information, if I think that's anywhere closer to reality than my knowledge is, I'm afraid for the future. I really am.

Thank you very much, Mr. Campbell. It was a great presentation, with lots of good information exchanged. We appreciate the work you did in putting everything together to give us good answers and good information.

Mr. A. Campbell: Thanks for the opportunity. All the best.

The Chair: Thank you very much.

Our next presenter is right on schedule, and I will now give him an opportunity to take a chair. We haven't forgotten about you, Mrs. Forsyth.

Mrs. Forsyth: Okay, Barry. Thanks.

The Chair: We're now going to call on Mr. Paul Pellis, Deputy Minister of Service Alberta.

Mr. Pellis: Good afternoon, everyone. How is everybody doing today?

The Chair: Very good. Fresh from Thunder Bay.

Mr. Pellis: Actually, Ohio.

The Chair: Ohio. Okay. As with the previous one, Mr. Pellis, you've got 30 minutes for your presentation, and then we're going to open the floor for questions. For the record your name, your title. I don't know if Ms Blakeman wants to introduce herself to you.

Ms Blakeman: I just had a question before we start. Was your information that you're about to present made available to us on the website, and if not, do you have copies today?

Mr. Pellis: No on both counts, but I will absolutely make that available to you. I'll do that through the chair?

The Chair: You betcha. To the committee clerk would be just fine.

Mr. Pellis: To the committee clerk. Okay. Everybody behind me is taking good notes?

The Chair: They are.

Mr. Pellis: That's great.

The Chair: We understood that you were here to answer questions because you've got quite a familiarity with it, and your department is actually in control of freedom of information.

3:00

Mr. Pellis: That's what I'm told, Mr. Chairman.

The Chair: Thank you. Well, we look forward to the presentation.

Service Alberta

Mr. Pellis: First of all, Paul Pellis, Deputy Minister of Service Alberta. I've been with the department now for five years. I'm attending the meeting today to provide information and answer questions about the relationship between the FOIP Act and information technology developments, contracting, and information sharing.

Before I get into some specific topics that this committee has raised, I wanted to take a moment to talk about the role of Service Alberta as it relates to the FOIP Act. Simply put, Service Alberta is responsible for setting policy and guidelines for government regarding the freedom of information and the protection of privacy. The onus is on each public body to ensure compliance, and the Privacy Commissioner is generally responsible for monitoring how the FOIP Act is administered. The FOIP Act itself is designed to be technology neutral. It reflects a set of principles which in theory can be broadly applied to any kind of information or records.

As we're all aware, technology is a rapidly developing field. All governments are striving to utilize new technology developments as quickly as possible, particularly in areas where we can better service the public and reduce our costs. With the dynamics of changing technology it's important that legislation be principle based with a strong focus on standards.

The next thing I want to talk a bit about is cloud computing. One of the innovations that's challenging public bodies today is the concept of cloud computing. Traditionally computer applications and electronic document storage have resided on a user's workstation or secure computer network. To prepare a document in Microsoft Word, Word must first be installed on a user's computer. Once a user has completed working on a document, it is stored on a user's computer or on a secure network.

Cloud computing is a different approach. In one version of cloud computing file storage, e-mail, and other computing applications are managed by third-party providers. Applications do not reside on an individual's laptop or computer. Applications are accessed via the Internet or on servers operated by a third-party provider. For example, as an alternative to buying Microsoft Office software, Google currently offers free online applications for word processing, spreadsheets, and presentations. The use of online computer applications is often referred to computing in the cloud.

You may wonder: why would a public body consider using this type of cloud computing? The most significant advantage is decreased costs. In some cases services are free. In others services are billed on a consumption or subscription basis. The use of this open type of cloud computing can eliminate the need for software licences, upgrades, and other significant costs. Services can be accessed anywhere, at any time, and from any computer.

Recently, as many of you are aware, the University of Alberta decided to adopt Google's Gmail for all staff and student mail. To address access and privacy concerns, the university conducted a privacy impact assessment, which was reviewed by the Information and Privacy Commissioner's office.

Unless appropriate mechanisms are in place to restrict access to information residing in the cloud, it should be assumed that all stored data may be accessible by the cloud service provider and visible to outsiders, even if only by accident. The GOA ensures that

there are appropriate and robust terms and conditions in all of our contracts, and I'll provide you with details when I talk more specifically about GOA contracting.

There are several issues a public body needs to consider in relation to cloud computing. The FOIP Act requires a public body to make reasonable security arrangements to protect personal information from risks such as unauthorized access, collection, use, disclosure, or destruction. The ability of a public body to protect personal information processed and stored in the cloud is challenging because in the most open form of cloud computing users generally do not control the underlying cloud infrastructure, including network, servers, operating systems, storage, or application capabilities. Information is processed and stored on multiple servers in different locations, often in countries that may not have privacy laws that are as strong as Canada's.

Unless appropriate mechanisms are in place to restrict access to the information residing in the cloud, it should be assumed that all stored data may be accessible by the cloud service provider and visible to outsiders. This is of particular concern when the information is personal information. Some have argued, however, that cloud service providers such as Google are at the cutting edge of technology and may be able to provide more robust security than would otherwise be available to an individual public body.

The basic objectives of the FOIP Act are to ensure that public bodies are open and accountable to the public by providing a right of access to records and to protect the privacy of individuals by controlling the manner in which public bodies collect, use, and disclose personal information. The act applies to records in the custody or under the control of a public body. A public body has custody of a record when the record is in the physical possession of the public body. A record is under the control of a public body when the public body has the authority to manage the record, including restricting, regulating, and administering its use, disclosure, or disposition.

Because the FOIP Act is technology neutral, any recorded information which is in the custody or control of a public body is a record for purposes of the act regardless of the media format. In other words, a public body must comply with the FOIP Act's rules regarding access and privacy whether the information is paper records, electronic records, or the method of storage by way of traditional desktop network-based computing or electronic records processed and stored in a cloud. When using any new technology, the public body is responsible for ensuring that it continues to meet its obligations under the FOIP Act.

In traditional client-vendor contracts a public body can include specific accessing and privacy clauses and provisions. However, a cloud user may be required to agree to the service provider's boilerplate terms and conditions. The only option to the user in these instances is to agree to the terms or simply not use that service.

Another concern is that the merger or acquisition of cloud service providers may unilaterally change the operating rules of the cloud itself. For example, a provider may be bought out by another organization that has a different privacy framework or culture with policies and procedures that do not meet the standards of the public body. Similarly, information may be at risk if a provider ceases to operate or goes into bankruptcy. An example would be that the information that's held by the provider would be considered an asset of that provider.

The FOIP Act does not say that a public body can or cannot use cloud computing services. It does say that public bodies need to be able to provide access to records and protect privacy, and this responsibility applies whether or not it uses cloud computing services.

Remember, I mentioned earlier that I was speaking about one version of cloud computing. That was the totally open environment. But there is another version, a more private version, and we call it a GOA cloud computing environment. Under this version we take advantage of the very robust computer capabilities under the care and control of the GOA. The government believes that this version has advantages in terms of server-sharing and cost-saving opportunities. Work is currently under way to pilot this version, keeping information internal to the GOA's secure computing environment and ensuring compliance with FOIP.

So really what we're saying here is that what the GOA is looking at right now – and it is still a pilot – is that we've got a lot of computing capability which is under our care and control. We think that we can look at a version of cloud computing that addresses our security requirements and addresses our privacy issues as well. Similarly, cloud computing may be used while remaining in compliance with the FOIP Act where contracts are tightly constructed and managed, services are appropriately reviewed to ensure compliance, and if user consent is obtained where required. I'll elaborate on some of these measures in a few minutes.

The next point that I want to talk briefly about is online social networking. Another challenge that public bodies face is the use of online social networking sites such as Facebook and MySpace. A social network is a community made up of individuals who are connected by a shared characteristic such as friendship, kinship, hobbies, or profession. Online social networking allows these connections to take place over the Internet. Once granted access to a social networking site, a user creates a personal profile or page, which allows him or her to meet, gather, and share information with others.

The most popular social networking site right now is Facebook. In the last six years Facebook has grown from a small online community for college students to over 500 million active users worldwide. People using social networking sites stay connected with friends, family, and people with common interests or for business networking. Online social networking is not just about teenagers and young adults. In fact, 58 per cent of users are between the ages of 35 and 44. Organizations, including public bodies, may use social networking sites to reach a particular audience or demographic. For example, a university may create a Facebook profile to reach potential students who also use Facebook. Organizations may also use social networking sites to connect employees that may be in different locations or offices and to communicate with the public.

3:10

When a public body creates its own profile on a social networking site or uses information from a site, the public body is responsible for ensuring that its actions comply with the requirements of the FOIP Act. There are several issues that arise when a public body is considering using a social network site for service delivery. The FOIP Act allows public bodies to collect personal information only when the collection is authorized by legislation or is for law enforcement purposes or when the information relates directly to and is necessary for an operating program of activity.

If a public body is collecting personal information via a social networking site – for example, let's say they're inviting comments about a program or service – it may be difficult to control that collection. An individual may post more and very highly sensitive personal information than what the public body would otherwise be permitted to collect. When personal information is collected directly from an individual, the public body must inform the individual of the purposes for the collection and the specific legal authority for that

collection. It must also provide the contact information of an employee of the public body who can answer questions about that collection. A public body may have limited ability to incorporate such a notice on its social networking page.

Another concern is that public bodies can collect personal information from someone other than an individual which the information is about only under circumstances permitted by the act – these include consent – and where authorized by legislation. An individual's response on a public body's page may include personal information about other individuals when the public body may not have the authority to collect that information.

Also, the FOIP Act requires public bodies to protect personal information against risks such as unauthorized access, collection, use, disclosure, or destruction. Servers for social networking sites such as Facebook are typically located outside of Canada, for the most part in the United States. Privacy policies for many social networking sites change frequently and without warning and may not be consistent with the requirements of Canada's privacy legislation. Many sites permit secondary uses of information posted to the sites for marketing or other commercial purposes. Privacy assurances can be difficult to make to individuals visiting a public body's profile or social networking page. Public bodies must determine which information on its site needs to be captured as a permanent record and how it will do so in order to provide access to it in the event of a FOIP request. Consideration must also be given as to whether content can be permanently removed from a site or merely deactivated and how this fits in with the public body's retention and disposition schedules.

A public body must also examine the degree of control it has over the subsequent use of content. The terms of use of many sites give the site provider the right to use information submitted to the site for the provider's own purpose. For example, the terms of use for YouTube give YouTube broad legal rights, including the right to reproduce, sublicense, and distribute any materials posted on its site.

You can see from that that there's a fairly lengthy list of issues to deal with. Again, the FOIP Act does not say that a public body can or cannot use social network sites. It does say that public bodies need to be able to continue to provide access to records and ensure that privacy is protected.

To summarize, personal information provided or posted directly by individuals to an official GOA social media page channel site can only be collected by the GOA for reference or subsequent use if that information is necessary for an operating program or the collection is otherwise authorized or required by law. All GOA social media channels that are intended to collect personal information about visitors or contributors for program purposes must display a notice of collection in accordance with the FOIP Act. In its social media post the GOA also promotes the protection of citizens' privacy by including links to the GOA, Information and Privacy Commissioner, or other information about how to protect one's privacy when using social media. A record posted by GOA employees to a social media channel moderating activities and responses must be maintained in the ministry's official record keeping system and must be subject to a records retention schedule.

The next thing I want to talk about a little bit is contracting and the FOIP Act. Public bodies may hire contractors for a variety of purposes such as program delivery, information and communication technology functions, data processing, and storage. Once again, public bodies need to continue to provide access to records and protection of privacy when using the services of a contractor. The FOIP Act applies to all records that are in the custody or control of a public body. When a public body uses a contractor, the records may be in the office of the contractor, but the public body maintains control over the records because they relate to a service performed by the contractor on behalf of the public body. Control means a public body has the authority to manage the record, including restricting, regulating, and administering use, disclosure, or disposition.

The definition of employee in the FOIP Act expressly includes "a person who performs a service [on behalf of] the public body." This means that those provisions in the act which refer to an employee apply to individuals or organizations that perform services for a public body under contract. For example, the act permits a public body to disclose personal information to an employee of a public body if the disclosure is necessary for the performance of the duties of the employee. This allows a public body to disclose personal information to a contractor in order for the contractor to provide the services outlined in the contract. In most cases the act does not specifically refer to the employees of a public body. Public bodies must therefore control the actions of contractors through the terms and conditions of the contract. Contractual provisions are put in place to ensure that public bodies can continue to meet their obligations under the act because a public body cannot contract out of its obligations under the FOIP Act.

As I alluded to earlier, when personal information crosses jurisdictional boundaries or where the laws of another jurisdiction apply to a public body's contract, there is concern that a court in another jurisdiction may order the disclosure of personal information. This issue came to public attention with the passage of the USA PATRIOT Act following the September 11 attacks in the United States. That act allows the U.S. Foreign Intelligence Surveillance Court to issue secret orders permitting U.S. law enforcement agencies to gather information about individuals from U.S. service providers. Failure to comply with an order and to keep its existence secret is an offence in the U.S.

In Alberta the FOIP Act was amended in 2006 to specifically address the issue of orders from foreign courts. The amendments clarify that a public body may disclose personal information for the purpose of complying with a subpoena, warrant, or order only if the issuing court or tribunal has jurisdiction in Alberta to compel the production of information or if a rule of court binding in Alberta requires production of information. It is an offence to contravene this nondisclosure provision, with fines between $2,000 and $10,000 for an individual and $200,000 to $500,000 for any other. The substantial penalties ensure that a contractor considers the serious consequences of unauthorized disclosure if it receives a subpoena, warrant, or order from a court who has no jurisdiction in Alberta. In addition, the offence and penalty provisions signal to other jurisdictions the seriousness with which Alberta takes contravention of its own privacy legislation.

The government of Alberta has many contracts with service providers. We have developed standard procurement and contract templates that are used by all GOA ministries. These templates also cover all of our IT contracting. The standard templates include provisions to ensure full compliance with the requirements of the FOIP Act. I think that what I'm going to do now is read some of the clauses just for the record. I think it's important to articulate the number of clauses that we do have in place in our contracts to ensure that contractors comply with the FOIP Act.

3:20

The first part deals with the Freedom of Information and Protection of Privacy Act, and it reads:

> 2.4.1 The Vendor acknowledges that:
>
> (a) The Freedom of Information and Protection of Privacy

Act of Alberta . . . applies to all information and records relating to, or obtained, generated, created, collected or provided under, the RFP or the Contract and which are in the custody or control of Her Majesty. FOIP allows any person a right of access to records in Her Majesty's custody or control, subject to limited and specific exceptions as set out in FOIP;

(b) FOIP imposes an obligation on Her Majesty, and through the RFP and Contract on the Vendor, to protect the privacy of individuals to whom information relates. The Vendor shall protect the confidentiality and privacy of any individual's Personal Information accessible to the Vendor or collected by the Vendor pursuant to the RFP or the Contract;

(c) The Vendor, if it considers portions of its Proposal to be confidential, shall identify those parts of its Proposal to Her Majesty considered to be confidential and what harm could reasonably be expected from disclosure. Her Majesty does not warrant that this identification will preclude disclosure under FOIP.

(d) Materials produced by the Vendor, in connection with or pursuant to the RFP or the Contract, which are the property of Her Majesty pursuant to the RFP or the Contract, [are] considered records under the control of a public body and could therefore also be subject to the FOIP before delivery to Her Majesty. As such, the Vendor must conduct itself to a standard consistent with FOIP in relation to [all] such Materials.

(e) For the records and information obtained or possessed by the Vendor in connection with or pursuant to the RFP or the Contract, and which are in the custody or control of Her Majesty, the Vendor must conduct itself to a standard consistent with FOIP when providing the services or carrying out the duties or other obligations of the Vendor under the RFP or the contract.

2.4.2 Prior to the start of the Services by the successful Vendor, the Vendor must provide a detailed plan describing the security measures to be implemented to ensure the protection of personal privacy and to ensure that only those employees, subcontractors and agents of the Vendor who are required to have access to, or to collect, Personal Information for the purposes of providing the Services and Materials required under the Contract, are permitted access to that Personal Information. The plan shall address the [standard] requirements, as appropriate for the Proposal [including]:

(a) manner of collection;
(b) notification of collection purposes;
(c) assurance of accuracy;
(d) plans and controls over data matching and linkage;
(e) controls over uses and consistent uses;
(f) controls over disclosure of Personal Information;
(g) provision for retention and disposal of Personal Information;
(h) protection of Personal Information from unauthorized access; and
(i) collection, use . . . or disposal.

2.4.3 The purpose for collecting Personal Information for the RFP is to enable Her Majesty to ensure the accuracy and reliability of the information, to evaluate the Proposal, and for other related program purposes of Her Majesty. Authority for this collection is the Government Organization Act, as amended from time to time. The Vendor may contact the Contracting Manager identified in the RFP regarding any questions about collection of information pursuant to the RFP.

I think I'll stop there. You can see that there are very specific, rigorous, and stringent provisions requiring that vendors protect the confidentiality and privacy of personal information made available to or collected by any vendor. Additionally, these provisions require that vendors develop a plan describing the security measures that will be implemented to protect personal privacy. All significant contracts are reviewed by legal services to determine whether additional provisions concerning FOIP may be required from time to time.

I'd also like to point out that any noncompliance is subject to severe legal sanction, including but not limited to the penalties pronounced in the FOIP Act, contract termination, and any other legal ramifications.

Mr. Chairman, I think I'll stop there, and I'll open it up to any questions from the members.

The Chair: Well, thank you very much, Mr. Pellis. I appreciate the time that you've taken today.

We'll start with questions from Mr. Olson, please.

Mr. Olson: Thank you very much for the information. My colleague Mr. Vandermeer asked the last presenter a question that I want to ask you, and it has to do with – actually, I think you kind of referred to it when you talked about the government of Alberta cloud computing. Is it practical to think that we could accomplish all of this data management in Alberta and at the same time use it as a means of diversifying our economy and building something that we could sell, perhaps, to other jurisdictions? I need to be a little careful about talking about government getting into business, but it strikes me that there is a benefit for us in Alberta if we can keep this stuff at home, and if at the same time we can use it as a revenue stream for the province, that would be something worth considering.

Mr. Pellis: I believe that there absolutely are some value-added positions that the government could take, and I do believe that there are significant economic benefits possible.

A couple of points I want to make around that. I heard the previous speaker say that there was a policy in place with respect to storage of data, and he was unclear whether that policy was still in place and was adhered to. The answer is that there is still a policy. We do not store data outside of Canadian borders. We strongly encourage that data be stored in Alberta, but our default fallback position is that data must be stored in Canada.

With respect to the economic diversification piece, right now the government of Alberta is short on data centre space. We are busting at the seams. As more technology comes forward, as more initiatives come forward which require strong, robust technology platforms, we are going to need more space to do that. We are currently in the very early stages of considering putting out an RFP to look at data centre storage, and the perspective we're taking right now is a made-in-Alberta solution. We would like to see, if there are going to be new data centres built, if there is going to be data centre capacity developed, that as much as we can within the restrictions in place under TILMA and FTA, et cetera, we look at a made-in-Alberta solution. So I do think that there are definitely opportunities there.

I also want to be clear on the point that was made before, that our policy is that data is stored in Canada, with a preference for Alberta.

Mr. Olson: Thank you very much.

The Chair: Thanks, Mr. Olson.

Ms Blakeman: Just at the very end you were talking about the penalties that are in the act, which tend to be financial. I'm wondering if it is on your list of penalties and if it is used at all or a common practice to strike a vendor from a list of qualified vendors if they breach any of the contract and if you could give us an idea of how many times that's happened in, say, the last five years.

Mr. Pellis: Absolutely. We have that ability. I would like to point out that because our contract provisions are so stringent right now, we've never had to exercise that. I'm pleased that we've not had to, but if required, those abilities are absolutely there.

The vendors look at our contracting templates very seriously.

There are significant penalties in there for noncompliance, and I'm very pleased to report that all of the vendors we do business with today work very hard to ensure that they are fully compliant.

Ms Notley: Two points. First of all, I really have to compliment the MLA from Wetaskiwin-Camrose for his creative thinking about the role that government can play in economic development. He sounds like a member of my caucus.

Anyway, I would like to just follow up on the points you were making about the obligations of service providers to adhere to FOIP. As you're probably aware, we've been having discussions about the way in which that is or isn't different and the degree to which the obligations extend. I, of course, as you can imagine, am most concerned about access. I don't have a clear understanding. I don't want to say that I'm not getting a clear answer; I just struggle to get a clear understanding of how this is working. I do understand that service providers are treated like employees under the act; therefore, the obligations of an employee of a public body are passed on to the service provider. I guess what I'd like to know is: is there a different between the citizen's right to access information from a service provider versus the citizen's right to access information from, let's say, your ministry?

Mr. Pellis: I would say the answer to that is no. There is absolutely no difference, and there should not be any difference. If you recall, I know I was a bit long-winded when I went through the contract provisions, but I did that for a reason. The way the contracts are worded, the contractor is an agent of the government and subject to all policies, rules, and legislation of the government, including the FOIP Act, and we take that very seriously.

Ms Notley: So, then, when a contract is entered into with the service provider, is the contract itself accessible? Is that not a description of how public funds are being allocated and how they're being spent?

3:30

Mr. Pellis: You know, the reason that a contract may or may not be provided is, I would say, that most of the time, if not all the time, the contract includes very – how can I describe it? – I guess, proprietary information of how the contractor is delivering the services to the government. They take that very seriously, and they want to ensure that that information is kept only within the hands of themselves and the government.

I can remember a few examples where in the early days of FOIP we had a contractor who was unsuccessful on a bid, and he wanted to see the other individual's proposal. The department I was in at the time said no. If memory serves, it went to the Privacy Commissioner of the day, and he absolutely agreed with us because by the time we would have severed what was in that contract that was proprietary and secure to that individual in terms of how they were delivering the service, there wasn't much value left in terms of providing it.

A lot of times the information that is not specific to the vendor is in the RFP, which is a public document. Anybody can access an RFP and pull it down.

Ms Notley: Well, the RFP is your document. It's not the ultimate document.

Mr. Pellis: But the RFP forms the actual contract at the end of the day. The only thing that's not included in the RFP is the proprietary approach that the contractor chooses to use to deliver that service.

Ms Notley: Right.

Mr. Pellis: There's nothing to prevent someone from making a request under the FOIP Act, and if the individual in question is not satisfied that perhaps the public body released everything, that's certainly the role of the privacy commissioner in that regard.

Ms Notley: Right. Then arguably, since almost every contract is subjected to that proprietary exclusion, we're at the very least adding another step to the access.

Mr. Pellis: Except that, I guess I would wonder, outside of the specifics of how a company chooses to deliver a service or build something – let's say that we put out a contract to have a bunch of widgets built, and the contractor who won has a very unique process that they have patented to build that widget. I don't think that the Privacy Commissioner would then say to those people: well, you spent all the time and money and got a patent, but I'm going to authorize release of that information.

In terms of the contract itself 80 per cent of that contract is in the RFP.

Ms Notley: Right now, for instance, you know, we have the blue book process, where ultimately we can go into that blue book, and absolutely every person, agency, body, whatever who gets a public dollar is listed. If that public dollar – let's say in the case of Alberta Health Services 13 billion public dollars – goes to an agency, then that's where it stops. We don't get to go, then, to that agency. Perhaps Alberta Health Services isn't the best example. But we don't get to go to that private agency and say: we want a blue book level of accounting of where your money has gone. Right?

Mr. Pellis: I guess I can only comment for the government of Alberta and that, you know, the blue book does provide full disclosure of the vendors who we deal with. I'm not in a position to comment on how Alberta Health Services operates.

Ms Notley: Right. I guess that's my point, though: we get that information from fully public bodies; we don't get it once we contract out that service. The vendor to whom we contract does not give us the same level of detailed accounting of where our dollar has gone.

Mr. Pellis: Can I ask in the sense of if there was a contract with a third party, and the RFP was totally available to the public – and it is for anybody to download – what piece of information is missing? That's what I'm trying to get my head around. What's missing in that situation?

Ms Notley: Well, because we're not seeing exactly how they're spending the money to meet the terms of the RFP.

Mr. Pellis: But you do understand that in those cases we want 15 widgets built, and somebody won the contract to build 15 widgets. At the end of the day, in addition to all of the other terms and conditions of the contract, there has to be 15 widgets delivered.

Ms Notley: Right. But the fact of the matter is that we may want to know how those 15 widgets were delivered, who participated in delivering them, how much each widget production component cost. That's what accountability is. That's what transparency is. It seems to me that once you contract it out to a service provider, we start to lose that transparency.

Mr. Pellis: Okay.

Mrs. Forsyth: Mr. Chair, I'd like to ask a question if you could put me on the list, please.

The Chair: I have you on the list, and it'll be after Ms Pastoor, who's up right now.

Mrs. Forsyth: Thank you.

Ms Pastoor: Thank you. You had mentioned the contractual rules,

and we've sort of had a bit more of a conversation on that. I think, as we all know, rules on paper look great. How are these rules monitored? How are they enforced? In fact, is it only on a complaint basis that somebody would actually look at if these contracts are actually being delivered as promised?

Then, also, you've said that all of our information is stored in Canada, but how many companies or people outside of Canada actually have access to those records? I'm sort of thinking of IBM, that would have set up some of these systems in the first place.

Mr. Pellis: First of all, your question about compliance with contracts. We do have contract managers in place. If it's an overall GOA contract that covers many ministries, that contract management skill and responsibility rests with Service Alberta. If there are individual contracts with work specifically undertaken for one department, that contract management expertise rests with that department. So there are continually checks and balances in place; there are continually checks put in place on that.

In addition to that, as one of the offices under the corporate chief information officer we have a chief security officer who also looks at those aspects as well to ensure compliance because, as I think you can appreciate, if you have very robust, rigorous terms and conditions but they're not enforced, they're not worth the paper they're written on. So we take that role very seriously, and we do ensure full compliance.

With the question about third-party data, or GOA data that may be in the hands of a third party, I go back to the terms and conditions of the contract that I read to you. One of them was – and it was kind of legalese again, but really the essence of that clause is that it's on a need-to-know basis. The only people who should access that information are those that need to know that information for purposes of performing their duties under the terms and conditions of the contract. Again I'll tell you that our contractors take that very, very seriously.

The question was asked about a vendor being taken off our preferred list. They know that they want to stay and have the opportunity to bid on government jobs, and one of the ways of doing that is to ensure that you're fully complying with the terms and conditions of the contract.

Ms Pastoor: I guess what I sort of had in mind was the PATRIOT Act because, I mean, anything that the States decides that they need to know, they need to know.

Mr. Pellis: But if the data is in Canada, it won't be subject to that. If you remember, one of the other things we did is that we amended our FOIP Act to ensure that any judicial matter that comes forward has to have standing in Alberta, and the PATRIOT Act does not have standing in Alberta. So if the data is in Canada, number one. Number two, if somebody in Louisiana or California or Nevada or where I just came from, Ohio, wants to do something with IBM, the data that's in Canada is off limits completely.

Ms Pastoor: Thank you.

Mr. Pellis: You should know that I think just when the PATRIOT Act was first introduced, around 2001 – I happened to be just getting into the department – we did have a major contract where not primary data but, I believe, backup and recovery was in the U.S., and we asked that that be moved to Canada right away.

I also want to say that I think that we've got to be careful about what is the ultimate objective. I firmly believe that the objective of the FOIP Act is to ensure that information is secure and that if it's private, it's kept private. That has to be the objective because I think there's a risk if we say: well, if the data is in Canada, it's all good. I think it has to be more than that. Security is paramount. We've got hackers all over the world that try to get into it. You made the comment about the Pentagon.

You know, I talked about the chief security office. We now run a 24/7/365 monitoring operation, every day, all day, all the time, and any issues that come up are immediately reported and escalated. We do that all the time. We're trying to stay ahead of the game. It's hard at times to do that, but it's important, and it's critical that we do it. I'd suggest that we've probably got one of the best security regimes in Canada right here in Alberta because we take this matter very seriously and we've put a lot of time and effort into ensuring that the data is secure.

3:40

Ms Pastoor: Thank you.

The Chair: Thanks, Mr. Pellis.

Mrs. Forsyth.

Mrs. Forsyth: Thank you, Chair. We've had various presentations today – one from Alberta Press Council, the other one B.C. Freedom of Information and Privacy Association – that were sharing some of their concerns with us in regard to the public having the right to be informed, the barriers that they've seen. I want to give you two scenarios, and then maybe you can tell me. Both of them warned about the contracting private bodies that are not falling under the act. Examples were used. One of them is that Alberta children's services contracts with a private group home and not being able to access the information because the group home is indicating that they don't fall under the act. Another situation is that Alberta Health and Wellness contracts with Alberta Health Services, and Alberta Health Services then contracts with a private provider. Who or how do you FOIP to get the information you want, especially when, for example, under children's services it goes to the group home? In the second scenario it's gone from Alberta Health and Wellness to Alberta Health Services to a private contractor.

Mr. Pellis: Yeah. I'm not familiar with the specifics of either contract, but I'll say that if this was a matter that was brought to Service Alberta prior to entering into a contract, I would say that the way you address this is with robust and rigorous terms and conditions in the contract. We've never had a situation with any of the contracts that we've administered in Service Alberta where we've had an issue under FOIP because we're very diligent in ensuring that the terms and conditions fully comply with the FOIP Act and that the contractor clearly understands that they must comply.

As I said, one of the things we ask contractors to do is put together a security plan for us, that we review in advance of signing a contract, where they demonstrate to us very clearly how they're going to comply with the FOIP Act. That would be the general answer I could provide because I'm not familiar with the specifics of those two contracts. We'd have to have a look at what the terms and conditions are in there.

Mrs. Forsyth: So if children's services contracts with a group home, is their contract looked at by you at Service Alberta so that all of the rules and regulations and everything are followed?

Mr. Pellis: If somebody were to come to us and say, "We'd like you to work with us on a contracting template that is compliant with FOIP," essentially the piece that I read in my remarks would be what we would strongly recommend be included in any contract with a third-party provider. What I can't comment on is specifically whether or not either of the two contracts you referenced specifically have those clauses.

Mrs. Forsyth: But you indicated earlier that the contractors are all agents of the government and subject to all the rules.

Mr. Pellis: Correct. But that's included in the Ts and Cs of the contract. Where the authority comes to stipulate that is in the

contract itself, which is signed by the government and by the service provider, whoever he or she may be.

Mrs. Forsyth: Then they should be all subject to the same.

Mr. Pellis: As long as the terms and conditions of the contract include that. Again, I must apologize. Not having the specific contracts, I can't make any specific comments in that regard.

Mrs. Forsyth: Okay. Well, I just go back to the fact that you said that the contractors are all agents of the government and subject to all the rules.

Mr. Pellis: And the method of doing that is by putting those terms and conditions in the contract that both parties sign.

Mrs. Forsyth: Well, that's what I mean. But if they're all subject to the same rules, why aren't they signing the same terms and conditions?

The Chair: Heather, we'll have to get a clarification. If you can forward that request to Karen.

Mrs. Forsyth: Sure. Well, Barry, if I may, that was one of the submissions by the Alberta Press Council; that was one of their frustrations. I'm trying to follow that up.

The Chair: Right. I'm not saying . . .

Mrs. Forsyth: I'm just trying to get clarification from the deputy minister.

The Chair: But I think he's tried to indicate, you know, that he's aware of what happens in Service Alberta, but if Alberta Health Services or Alberta Health and Wellness have a contract that's any different – I guess we're going to have to get your question and Alberta Press Council . . .

Mrs. Forsyth: I'm not arguing with you, Mr. Chair.

The Chair: No, I know.

Mrs. Forsyth: I'm just referring to a comment that the deputy made when he said that all contractors are agents of the government and subject to all of the same rules. That's my comment.

The Chair: Okay. Well, we're going to get the research people here on it, and we'll develop some answers for all the committee, besides yourself.

Mrs. Forsyth: Yes. You know, the other thing he mentioned was that the government of Alberta has many contracts, and they're all standard templates for all the departments.

Mr. Pellis: No. If I can clarify that, Mr. Chairman. We provide a standard template. Departments have the discretion, if they so choose, to change that template to meet their specific requirements. To say it differently: we are not the contract police in Service Alberta. Our job is to provide sound advice, counsel, and we ensure as much as we can that everybody adopts what we consider to be best practices. But at the same time we have to be cognizant of the fact that individual public bodies may change the terms and conditions of a contract to meet their specific program requirements, and I'm not privy to why they would change or adjust a contract to meet those program requirements.

An example I can give you is that we talked about in my opening remarks the fact that the University of Alberta went to Gmail, and apparently, reading the press releases of the time, they went into some very specific contracting provisions with Google to ensure that the privacy provisions were met. I don't know how they did that. Now, they probably did that on their own and did what they felt was in their best interest. They have legal counsel and everybody else that provides them good advice.

The Chair: Would it be fair to say, Mr. Pellis, to answer Heather's question in a different way, that if it was government policy that your template would be used by all departments, then you could safely say, "Yes, I know without doubt that what we are doing in Service Alberta is what is happening in children's services, in health services, or whatever"? But until that becomes policy, you would be the sole source or template. Is it correct to say that?

Mr. Pellis: That's correct, Mr. Chairman.

The Chair: Okay. We've got one more, but I would like to kind of follow up. Remember, committee members, when Mr. Campbell made a comment about the cloud . . .

Ms Pastoor: Cloud computing.

The Chair: Right.

. . . and privacy impact assessments, and he suggested mandatory impact assessments be done? My information from the committee clerk was that if a group asks that a privacy impact assessment be done, there is a $25 fee or something along that line.

Ms Mun: If I may clarify.

The Chair: Yes.

Ms Mun: What it is is that if somebody wants to FOIP for a privacy impact assessment that has been completed, there's a $25 application fee.

The Chair: What I would like to ask just along the lines of the impact assessment: in your opinion as the deputy in Service Alberta, if that were to become a recommendation, that there be impact assessments done prior to any of this cloud survey stuff, whatever it's called, should that cost be borne by the proponent, or should it be borne by the Alberta government via the taxpayer?

Mr. Pellis: Well, if I go back to what I would consider to be one of the main reasons to consider cloud computing – and that is reduced costs – I think that if a public body such as the University of Alberta made a conscious business decision that they believed there was a value proposition in moving to cloud computing and in this case Gmail, the full cost of going to that decision has to be borne by the public body. If not, it's not really a valid business case, and you're not including all of the costs of the decision . . .

Ms Blakeman: And the risk.

Mr. Pellis: . . . and the risk that goes with it. Exactly.

Right now, Mr. Chairman, I do not think that the government of Alberta would consider in any way, shape, or form moving to a third-party provider of e-mail. I think that we would look at it today and we would see significant privacy and security risks. If the technology improves, if the level of satisfaction increases significantly with respect to privacy and security issues, I do believe that that would warrant consideration but, again, very carefully because I think that the cost savings may come with a very significant risk, which could more than mitigate those cost savings.

3:50

That is why today you're seeing very, very limited, probably more than anything else pilot use of cloud computing outside of the GOA domain. If they were to come to us today to look at anything on a

broad scale, we would recommend against it simply because we believe that security and privacy issues outweigh the cost benefits that would be realized by moving to that environment.

The Chair: Thank you for that.
Now Dr. Sherman.

Dr. Sherman: Thank you. Mr. Pellis, thank you for your presentation. I think with all the clouds over Alberta over the last summer, all the privacy guys are going to be coming here anyways.

Mr. Pellis: Except it's a nice, sunny day here.

Dr. Sherman: You know, it was really reassuring to hear from Mr. Campbell earlier that legislationwise in the world we in Canada probably have amongst the best legislation – and we'll hopefully improve upon that now – and to hear from you how we're handling our data and handling it here in Alberta. My question to you is that cost is a big issue. Right now everything is done on paper. It takes time. It costs a lot of money. With the advent of technology and putting all our data on the computers, what do you see as the cost to ease of access for the public to information and at the same time the cost of protecting the information?

Mr. Pellis: First of all, on a point of storage, our storage costs are growing very, very significantly. While there is growth in our paper storage – and for anybody that's been out to the old Coronation warehouse on 142nd Street, it is absolutely incredible to go there. I think the ceilings are 30 feet high, and now they're stuffing the boxes in between the rafters. Anyway, that's paper storage, which is a big issue, and we need to address that, and we are trying to take a lead role on that in Service Alberta. Part of that is that we need to look at the classification of records, the retention, and also the disposition of records. We need to look at our policies, which probably were in place long before a lot of the technological advancements that are in place right now were there. We need to take a hard look at that.

The second thing. In the electronic world our data storage is also growing very significantly with the proliferation of e-mail, with data being stored through various mediums. Our data storage costs are going up significantly, and we need to take a hard look at that. For example, do we look at things like putting limits on the amount of e-mail that you can have at any one time; you know, we're going to give you 10 megabytes, and anything over that you have to start cleaning up your stuff? We've got to stop worrying about, you know, grandma's recipe for muffins being on an e-mail account in 15 places because it's a good recipe. I don't need to store that in the government of Alberta, but right now some of that stuff gets in there, right? Or somebody decides that there's an interesting video that maybe has some minor pertinent information for government and then starts sending it around, and then I've got 15 versions of a video file that I'm going to now store in my storage. We need to take a hard look at that, too.

The costs of storage are absolutely going up, and we're not alone in the government of Alberta. That's happening all over the place. The companies right now that make storage are making a lot of money because it's growing very significantly right across the board.

Dr. Sherman: Okay. Can you just . . . [A timer sounded] Are we done?

The Chair: I'm sorry. You can get it on the record, but there won't be an answer. He can get back to us.

Dr. Sherman: Can you guide us in the decision we have to make? One is to want to protect privacy. The second is to allow people more access and more freedom to more information and to allow more people access to more information. The more information we're going to have, that's a lot of work.

As to resourcewise, what kinds of resources will be required? We have to make these decisions. We've been asked to make it easier for many people to get more information quickly. How do you see the cost rising? Exponentially? I don't know if there's an absolute number with those requests.

Mr. Pellis: Some of the things that we're doing as a GOA community through the CIO council and others is important. We are starting to look at information from a GOA perspective as opposed to a departmental perspective. You look at the social-based assistance project as a good example. We're involved in a periphery from a technology perspective. But as far as we're concerned, if there is an Albertan that's in need of government services, their tombstone information should be recorded once. It shouldn't be recorded seven times and, unfortunately, differently so that, you know, there is no linkage. We should have that tombstone data once. The individual in question, if they need services from government, should look at it from a one-window perspective and not have to say: "Okay. I need glasses. I have to go to department X. I need financial support for some children that I have. I need to go to department Y."

The model that I think we're looking at trying to achieve is one window, where as far as the Albertan in need is concerned, the government is there to provide the services that that individual needs. Behind the curtain wall, if there's one department or five departments involved in providing those services, that should be invisible to them. The information requirements that we have for that individual we should collect one time, not five or six times. We need to do more of that.

The other thing we need to do is that if there are initiatives that cross departmental boundaries – I'll use an example of, let's say, Environment, Energy, and Sustainable Resource Development, that are looking at a place-based approach right now, that are looking at cumulative effects. We should be looking at that from one perspective as opposed to three. As soon as you look at it from three, you're storing the data three times, you're having to build bridges, you're having to build translations, and we need to look at trying to bring all that data together.

I do think that there's a lot of good thought going into this area right now. I think that we're going to make progress. It's going to take us some time. Also, I think we're not alone. This is not going to be an Alberta problem. I think this is a world-wide problem that's going on right now. I do think that we are going to make progress.

The Chair: Thank you, Mr. Pellis. I appreciate all the time and all the answers that you've given, and I know it's going to be helpful as we go forward with our final report and our recommendations. Thank you again.

Mr Pellis: Thank you very much. Everyone, have a good afternoon.

The Chair: You too.

Mr Pellis: Are you letting them out now, Barry?

The Chair: We've got one other brief thing here.

I just wanted to finish up on the other business that we discussed with Dr. Massolin. Based on the discussions we had this morning, I'm assuming that the committee is expecting that the research staff will complete a document identifying all the potential recommendations to be put forward and the issues that have been identified. If I'm correct in that assumption, then I'd suggest that this document should be available for the committee's review at least one week in advance of our next meeting, on September 27, if that's okay with everyone. Were there any other items along the lines of that research that we wanted to direct to Dr. Massolin and Stephanie and everyone else?

Mr. Groeneveld: Mr. Chairman, just a question on that for the research staff. Some of the stuff that we probably touched on today is very individualized. It doesn't maybe hold a lot of sway to where we're trying to get with this FOIP. I can see one tomorrow coming up as well. Do we make some kind of a decision on what they have to do with some stuff that maybe is not pertinent to where we're trying to get to?

Ms Blakeman: I'm trying to be careful here. I think that as we went through it, the submission that you're talking about that occurred today, there was something in it, actually. It just took ways of digging through it to find it. So I think we have to be careful about who will be the decision-maker on dismissing or putting something forward as a recommendation. I don't think we can place that burden upon the staff. I think it's just for them to collate everything they've seen, and we'll make the decisions about whether we proceed with it or not.

Mr. Groeneveld: I would agree with that. It's our decision, you know, what's pertinent. I think you would agree that there are some pertinent points in there, but maybe there's some stuff – I don't want to call it fluff – that probably doesn't pertain to what we're trying to deal with here.

Ms Blakeman: I think there was other jurisdictional discussion there that doesn't pertain to us, and I'm sure they'll be able to pull that out.

Mr. Groeneveld: Exactly.

The Chair: It'll be identified, and the committee will decide on the direction then.

Mr. Lindsay.

Mr. Lindsay: Well, thank you, Mr. Chair. I was just going to comment as well that I think, you know, that's the role of the committee, to listen to the presentations and decide amongst ourselves what's pertinent to the task at hand and what isn't. I agree that one was kind of moving around all over the place, but at the end of the day he did make a comment that is worthy of looking into.

4:00

The Chair: So we've got adequate direction for Philip and Stephanie?

Mrs. Forsyth: Barry, if I may. I know the day is long and people are tired, but they seem to be moving away from their microphones again.

The Chair: Okay. We were just making sure that Philip and Stephanie have got adequate ideas of what the committee expects to have come back at least a week before our next meeting so that we can review all the identified issues and potential recommendations.

Mrs. Forsyth: Okay. Thanks.

Dr. Massolin: Right. Mr. Chair, if I could summarize to make sure that we've got the direction. I think we do. Basically, what we've been tasked with is to prepare a compilation document of all the issues/recommendations that have come up to this point in the committee's proceedings from the written submissions, for example, from the oral submissions, the stakeholder submissions, and so forth. We'll put together that document. The document's purpose, basically, will be to serve as a guide as to what has been sort of presented to date, and the committee can use that as a background document, informing them for their deliberations the next time around.

The Chair: Correct. Sounds good.

With that, folks, thanks for your attentiveness today. We'll look forward to meeting tomorrow morning bright and early at 9 o'clock. Do we need a motion to adjourn?

Mrs. Forsyth: I'll make a motion to adjourn, Barry.

The Chair: Thank you, Mrs. Forsyth. All in favour? Carried.

Good night.

[The committee adjourned at 4:02 p.m.]

Published under the Authority of the Speaker
of the Legislative Assembly of Alberta