Title: Wednesday, June 27, 2007 PIPA Review Committee
Date: 07/06/27
Time: 9:32 a.m.
[Mrs. Ady in the chair]

The Chair: We're going to go ahead and call the meeting to order. I know that we have one more member joining us shortly, but we've got a fairly full agenda today, so I want to get busy if we can. I'd like to welcome everybody for coming out on this beautiful, slightly windy summer day.

I would ask if someone would move to adopt today's agenda, please. Have you had a chance to look at the agenda? It's pretty full.

Laurie Blakeman.

Ms Blakeman: Yeah. I just have a concern. This is no comment on our very hard-working staff; please, let met be clear about that. The background information was not available until Monday at about 10 o'clock in the morning, so we've had less than 48 hours – and I'm sure everybody had packed schedules – to try and work in the readings. So I am concerned about our ability to really give good discussion, coming from a knowledge base, for the agenda given that – well, perhaps everyone else is a faster reader than I, but I haven't been able to get through all of this. So I'm a bit concerned that we'd be making recommendations on behalf of the committee when we haven't been able to read the backgrounders.

The Chair: Any other committee members want to comment on this particular issue?

Mr. VanderBurg: We could always cancel the meeting and drive home, I guess.

Ms Blakeman: Well, I'm just thinking about how much stuff we can reasonably get through that people have been able to read the backgrounders on.

Mr. MacDonald: I would just like to support what Ms Blakeman has said. I don't think it's adequate.

Thank you.

The Chair: Now, I do know that, you know, we met last week, and the staff was of course trying very hard on Friday to get it all put together. So that's why it was posted as early as possible on Monday. Kind of has always been a bit of our schedule. So I'm prepared as chair to say that we need to move forward at this point in time. But I'll ask the committee, and it's up to them.

Committee? Anyone? All those in favour of continuing to move forward, who feel like they can move today?

Mr. Martin: We can always come back to it.

The Chair: Yeah. Laurie, as I said, if we don't get through it all – obviously, we might not – then we'll have to adjust. But we'll make a yeoman's effort to see where we can get today. How about that be my commitment at this point in time?

Are we okay? The committee has spoken; they have agreed.

I'll again ask for the adoption of the agenda. Ty. All in favour? Any opposed? Do you want that noted?

Mr. MacDonald: Yes, please.

The Chair: Thanks. That would be Ms Blakeman and Mr. MacDonald.

Okay. Moved that the agenda for the June 27, 2007 meeting of the Select Special Personal Information Protection Act Review Committee be adopted as circulated.

Now I need an adoption of the April 10 minutes. You have those in front of you. They're quite short.

Mr. VanderBurg: I'll make a motion that the minutes of April 10 of the Select Special Personal Information Protection Act Review Committee be approved as distributed.

The Chair: Any questions? All in favour? All opposed? That's carried.

Okay. We have some business arising from the last meeting. Members have a copy of the briefing document Non-Profit Organizations, or NPOs, which was provided by the office of the Information and Privacy Commissioner in response to discussion at our May 1 meeting. This briefing will come into play as we discuss issues related to nonprofit organizations further along in today's agenda. Is the committee agreeable to accepting this document with discussion and questions on it to hold until our discussion on question 7? Would you guys be in agreement to that, to holding this information until we talk about the not-for-profits on question 7? All those in agreement? Any opposed? Thank you.

Now, we'll move on to item (b). Item (b) is question 6D and a new briefing, application of PIPA to employees and officials. At our last meeting we tabled discussion of government recommendation 10. Now, that's from page 6 on summary of question 6. Question 6D is: "Should the definition of 'employee' be amended to clarify that all provisions of the Act that apply to 'employees' of an organization also apply to officials of an organization?" Ms Blakeman asked for additional information on the use of the term "employee" in the act, and we've just received this morning a briefing on the application of PIPA to employees and officials. You're getting it right now. I believe Jann is going to lead us through this discussion.

Ms Lynn-George: Just for some background, you'll find on the front page of this briefing a list of all the occurrences of the word "employee" in the act. It is defined in section 1, and then the term "employee" appears in the act's provisions relating to personal employee information; that is, information that's reasonably required by an organization for the purposes of establishing, managing, or terminating an employment or volunteer work relationship between the organization and the individual. Collection, use, and disclosure is permitted without consent for that relationship provided that the organization gives notice of the purposes.

It turns up again in sections 4(3)(c) and (d). These are cases where the act does not apply. The act doesn't apply to an organization's collection, use, or disclosure of personal information for an artistic or journalistic purpose, except where the personal information is personal employee information. What this means is that the *Edmonton Journal* can publish personal information without consent when it's writing a news article, but it can't publish information about its own employees without their consent.

The act doesn't apply to the collection, use, or disclosure of business contact information for the purposes of contacting an individual in that individual's capacity as an employee or an official.

PIPA includes a whistle-blowing provision, and that protects an employee who provides information to the Information and Privacy Commissioner about a possible contravention of the act.

Finally, in the regulation you'll find a provision that says that "an organization may not charge a fee to process a request for personal

employee information." So those are all the occurrences of that term "employee" in the act and also the term "official."

9:40

PIPA includes a broad definition of the term "employee." The reason why it's a very broad definition is that it allows an organization to collect, use, and disclose personal information that is reasonably required to establish, manage, or terminate a relationship between the organization and the individual who provides a service on its behalf. A person providing a service may be a traditional paid employee, but it may be another kind of individual as well, such as a volunteer or a participant or a work experience student.

That individual, even if he or she is not a traditional paid employee, is entitled to all the protections under the act. What that means is that even though they don't have the right to consent to collection, use, or disclosure of their personal information, they do have the right to notification about any collection, use, or disclosure of their personal information, they have the right to obtain access to that personal information at no cost, and of course there are the whistle-blower protections.

Now, the specific question here asked by Ms Blakeman was about how this would affect nonprofit organizations. The answer is that the protection for employees in the act has a very limited application to employees of nonprofits. I'm referring here to those nonprofits that are defined in PIPA. That's because PIPA applies to those organizations only when they're collecting, using, or disclosing personal information for a commercial activity, such as if they're selling or bartering a donor list, so very limited application there to nonprofits.

Since PIPA's definition of employee includes an individual who performs a service for an organization, it's quite likely that the provisions of the act that refer to an employee already apply to an individual who performs a service in a capacity other than the capacity of a paid employee. So if they're a director, a board member, a CEO, or they have some other similar role, they would probably be considered to be an employee for the purposes of the act.

But there's a problem. The act's provision for business contact information refers to an employee or an official, and that suggests, to the lawyers anyway, that an official is not an employee for the purposes of the act. So it's been proposed to try to fix this inconsistency. The government suggests adding "official" to the definition of employee and removing it from the provision for business contact information, really clarifying that your employees include officials as well as the other kinds of employees. Then business contact information covers the whole range.

The change would have a minimal effect on not-for-profit organizations under the act. Officials of not-for-profit organizations that are subject to PIPA – now I'm referring to those federally incorporated nonprofits, for example; there are others – are likely already included within the definition of employee, so there's no effect there. When we look at section 56 nonprofits, they're not likely to be affected either since the act currently has very limited application to the employees of those nonprofits.

Have I made myself clear?

The Chair: Yes. Thank you.

Ms Blakeman: I think this question needs to be looked at in the context of the other questions we have on our plate today because – and here's where you guys correct me because you're the experts – it doesn't appear to have much effect. But one of the other questions we have on our plate is about including all not-for-profits, no matter how they're designated or how we determine them, under this act. That takes away that strange category of commercial use that is so confusing. In that case, it does have a broader application, does it not?

Ms Lynn-George: In that case all the provisions that currently apply to organizations would apply to nonprofit organizations. Your employees of nonprofits, including officials, now are subject to those provisions that I described. So their information could be collected, used, disclosed for the purposes of hiring, managing a relationship, ending the relationship. But they would get notification, and they would have the whistle-blower protection, and they could get their information. They could make an access request and get their information at no cost. That's how it would apply on . . .

Ms Blakeman: So they actually get wider protection.

Ms Lynn-George: These are the protections that are afforded to employees. There is a no-consent provision when it comes to the handling of personal information for the relationship, exclusively for that relationship, and that's something that needs to be very clear.

Ms Blakeman: And that's 15, 18, and 21.

Ms Lynn-George: That's 15, 18, and 21.

Ms Blakeman: Okay.

Ms Lynn-George: It doesn't mean that any organization, nonprofit or otherwise, can disclose personal information about the officials, the paid employees, the volunteers for any purpose other than that relationship. I think that's a point that was not perfectly clear last week. There's just this sphere of activity in which there's an understanding that the employment relationship is special and that provided everybody understands the purposes for which information is going to be used, then you don't go back to get consent each time. You work on the basis of transparency in your operations.

Ms Blakeman: But you get notice, and you get access to correct.

Ms Lynn-George: Yes.

Ms Blakeman: Okay.

Ms Lynn-George: Well, everyone can correct it. The point is access at no cost.

The Chair: So, Ms Blakeman, are you more comfortable on this issue?

Ms Blakeman: Yes.

The Chair: Could we then move that

> the Select Special Personal Information Protection Act Review Committee recommend that the definition of employee be amended to clarify that all provisions of the act that apply to employees of an organization also apply to officials of an organization and that the provision for business contact information be simplified to refer to an employee of an organization.

Mr. Ducharme: Moved.

The Chair: Moved by Mr. Ducharme. All in favour? Any opposed? That carries. Thank you.

Now, we're going to be continuing our review of the responses received to each of the 13 questions in the discussion guide. But prior to doing that – I always forget to do this, to have everybody introduce themselves so that it can go on the record. I forgot last week, so I thought I'd remember really quickly this week. Is that everyone at the table? I'll begin with myself.

[The following committee members introduced themselves: Mrs. Ady, Ms Blakeman, Mr. Ducharme, Mr. Graydon, Mr. Lund, Mr. MacDonald, Mr. Martin, Mr. VanderBurg, and Mr. Webber]

[The following departmental support staff introduced themselves: Ms Kreutzer Work, Ms Lynas, Ms Lynn-George, Ms Swanek, and Mr. Thackeray]

[The following staff of the office of the Information and Privacy Commissioner introduced herself: Ms Clayton]

Ms Sawchuk: Karen Sawchuk, committee clerk.

The Chair: Thank you.

As you know, last time we met we got through questions 1 through 6. Today we will be doing and continuing questions 7 through 11. You have various documents included in your binders. Now, we are looking new. I notice that the committee is looking new but that the members all still have binders. That is the option. You can always have the material printed, or you could bring your laptop to these meetings in the future and not print your materials off. I, of course, have mine printed, I just want to point out. But that is the new step, the new stage. Again, next time that we meet, if you want to bring your laptop in and not have your assistants download this information, it's appropriate, and it'll be our new look on committees.

As you can see, Tom Thackeray and his staff have provided a summary and an analysis of the responses to each question as well as various briefing papers to assist the committee with primary issues related to each question.

9:50

We're going to move to question 7. It's the not-for-profit organizations. The first question concerns whether any change should be made to how the act applies to not-for-profit organizations. This is question 7 in the discussion guide.

We're going to follow the same process as the last meeting. Hilary Lynas will review the input from the public from the summary and analysis of responses, and then other staff will review the policy option papers provided on this topic. In addition, we will discuss the briefing on protection from liability that was distributed for last week's meeting. The committee is provided with options to consider with each issue paper, and a motion is required after each paper is presented.

I would ask the staff members if they can please keep their comments tight because this is going to take a little while. I know there's a desire to give us all the details that we need to make decisions, but again I just would ask you to keep your comments tight.

Yes, Laurie.

Ms Blakeman: Sorry. This is slightly administrative. Did we complete question 6E? We just did question 6D, which was that the definition of employee be amended to clarify, blah, blah, appearing on page 6 of the public consultation personal employee information document. Did we actually complete 6E? We didn't do it today. Did we do it last time?

The Chair: Just checking.

Ms Blakeman: Sorry. I just don't have it marked.

Ms Lynn-George: Our records say that that was . . .

Ms Blakeman: That was done? Okay. Good. Thank you. Sorry to disturb you.

The Chair: Okay. That solved itself. That's great. Thank you.

All right. We're going to be moving, as I said, to question 7. We'll have the summary and analysis from Hilary, please.

Ms Lynas: In terms of what the act says, PIPA includes nonprofits in the definition of an organization, but then later in the act section 56 limits how the act applies to certain nonprofit organizations. Three kinds of nonprofit organizations are singled out: those incorporated under the Societies Act and the Agricultural Societies Act and those incorporated under part 9 of the Companies Act.

The rules in PIPA are designed to protect personal information. They only apply to those nonprofit organizations I mentioned just a minute ago when carrying out a commercial activity. An example of a commercial activity is providing a service that would normally be provided by a business such as running a fitness facility. For greater certainty the act says that daycares, private schools, and private colleges are defined as carrying out a commercial activity.

When not carrying out a commercial activity, for example a local soccer club, the organization is not required to follow the rules for collecting, using, and disclosing personal information. Now, when you think about it, a local soccer club would have personal information about children, parents, volunteers, possibly board members, and paid staff.

An individual cannot make a request for access to his own information to one of these nonprofit organizations. The Information and Privacy Commissioner cannot investigate a complaint made against these organizations. In a few minutes Jill will provide some information on the commissioner's office's experience with complaints.

There are types of organizations other than those defined in PIPA who operate on a nonprofit basis. These organizations currently must comply with the act, and the Information and Privacy Commissioner can investigate a complaint.

Now, the comments that we have received about the question on nonprofit organizations have been divided into some categories. The first is on the inclusion of nonprofits under PIPA. Eighteen organizations and one individual indicated support for applying PIPA to nonprofit organizations. They stated various reasons but included that these organizations should be held to the same standard for protecting personal information and indicated that they were open to the idea of covering them.

One business commented that a large segment of society is served by nonprofit organizations. The business also stated that the privacy rules are confusing and impractical for nonprofit organizations because of the ambiguity over the concept of commercial activity.

One business commented that from the perspective of the individual the risks associated with inappropriate collection, use, and disclosure of personal information are the same regardless of whether the organization is a business or a nonprofit organization. This is especially true when the information is sensitive, for example medical or financial information.

One individual suggested that all organizations that are not subject

to the FOIP Act should be subject to PIPA. We do have a policy option paper on this issue, and we will present it in a few minutes.

Another group of comments was around the limited application of PIPA to nonprofits. One nonprofit organization said that PIPA should not be expanded beyond its current application, believing that repeated access requests or early disclosure of information could drain their resources and expose them to lawsuits.

Another organization commented that churches are not on the same footing as other nonprofit organizations. It suggested that any provision for nonprofits should apply to all religious organizations regardless of how and where they are incorporated.

Another organization stated that the current status should continue.

Another stated that condominium corporations are akin to societies and should not be subject to PIPA as they don't believe they engage in commercial activities.

One nonprofit noted that the exclusion of Alberta-based nonprofits from the scope of PIPA was at odds with the inclusion of federal nonprofits. Just a note: a federally incorporated nonprofit organization located in another province without private-sector privacy legislation wouldn't be subject to PIPEDA if it didn't carry out a commercial activity.

Two organizations and one association suggested amending the PIPA regulation to establish criteria qualifying an organization as a nonprofit under the act as the current definition excludes nonprofits that are incorporated under private acts or are incorporated or registered outside of the province.

Another professional regulatory organization recommended clarifying the definition of commercial activity to provide more certainty on whether fundraising activities of a society arm of school council could be considered commercial activity. We'd just note that Service Alberta has produced a publication for school councils and school fundraising societies regarding how PIPA applies to their activities.

One organization stated that all incorporated churches should have the same ability as congregations incorporated under the Religious Societies' Land Act to disclose a list of congregation members to members of the congregation. This issue is something we will cover in the policy option paper as well.

The Chair: Thank you.

As you said earlier, we're going to hear from Jill. Yes, Jill is going to give us a presentation on the statistics relating to not-for-profit organizations. So go ahead.

Ms Clayton: Thank you. I think Karen just handed out this information. At a previous meeting of the committee, members had expressed interest in receiving some information regarding what our office's experience has been with the not-for-profit sector. The information that is before you is about cases that involve not-for-profit organizations that meet the definition of a nonprofit under section 56 of the act.

Just by way of brief background, when our office receives a written complaint or a request for review, typically we do open a file unless it's obvious right up front that we don't have jurisdiction. With respect to nonprofit organizations, all told since the act came into force, our office has opened just about 730 case files at the time I pulled these statistics. Of those case files, complaints and requests for review, 31 of them had to do with nonprofit organizations as defined in the act. That's about 4 per cent of our total files. In 87 per cent of those cases, 27 of the 31, our office determined that we did not have jurisdiction. In pretty much all of those cases that was because there was no commercial activity, so the personal information was not associated with a commercial activity.

10:00

In four cases we did have jurisdiction. The types of activities there were training sessions that were provided on a fee-for-service basis that was comparable to other organizations, so that was determined to be commercial. We also found a complainant who was purchasing tickets for an event over the telephone from a nonprofit organization – that was a commercial transaction – and also an individual who purchased a product from a nonprofit organization. Those were very clearly commercial transactions, and we did have jurisdiction.

Where we've opened case files and either assigned them to a portfolio officer to investigate or where we may have opened a file and it was closed at intake after determination that there was no jurisdiction – I should point out that it's not always clear if we have jurisdiction over a nonprofit organization right from the get-go. Sometimes it requires a little bit of investigation to find out how the nonprofit was established because there certainly are organizations that operate on a not-for-profit basis but don't meet the definition under the act, and in some cases it takes a little bit of investigation to determine whether or not the activity itself is commercial. Certainly, that is a concern that comes up frequently if our office is presenting to nonprofit organizations. Their main concern seems to be that ambiguity over the definition of a commercial transaction: what is a commercial activity?

Of the files that we opened where we determined that we did not have jurisdiction, many of those were requests for access to information, so there was no right of access because there was no commercial activity. Also, there were some complaints about collecting too much personal information: the act requires that you limit collection.

We did have two self-reported breaches that are included in that number of 31 files. We did not have jurisdiction in those cases, but the nonprofit organizations reported the incident to our office. They were looking for some advice and guidance on how to respond to those breaches.

Typically, the kinds of organizations where we have received complaints have been either about employer/employee relationships, or we did have some complaints about social assistance organizations: disclosure of counselling information for example, one about a religious organization, residential associations, those kinds of organizations that are collecting information about tenants for example, or clients.

We have an intake officer who handles inquiries from the general public, and we typically receive probably around 200 phone calls and e-mail inquiries in a month. Of the requests for information – written, telephone, and e-mail inquiries – that we've received since the act came into force, just over 300 of those have to do with nonprofit organizations, or we could determine that the inquiry was about a nonprofit organization. Sometimes we don't know if the inquiry is by an individual or the nonprofit itself. Where we do know, they tend to split evenly. About half of the calls are from individuals; half are from nonprofits.

Typically, the kinds of questions that are being asked have to do with general application of the act – does the act apply in this case or not? – so jurisdiction questions. General questions about compliance: should we develop a privacy policy? Are there resources for privacy policies? What are best practices for safeguarding information? That is true when the inquiries have been made by nonprofits. They might be calling to say: "Can we do this? Is this an activity that would be regulated under PIPA?" Sometimes

they're calling to ask for clarification of what is a commercial activity.

In the stats that are before you on page 3, I just wanted to note that we've had seven inquiries by nonprofit organizations about collection and use of information, 42 inquiries about nonprofits on disclosure of personal information. Typically, what seems to be quite common is the idea of publishing personal information on websites, in newsletters, or distributing membership lists. Thirteen of the inquiries about disclosure of personal information had to do with whether or not the organization could disclose personal employee information. Again, that would not be a commercial activity, so we would not have jurisdiction there. Twelve of the inquiries by nonprofit organizations had to do with how to respond to requests for access.

Again, in almost all cases there would be no commercial activity associated with a request by an employee, or for that matter in some of the other cases we've had requests by parents for information about their children. Typically, that's a minor sports association, so a local soccer league. Parents are trying to access information. In these calls we're finding that the nonprofit was intending to respond to that request for access even though there might not have been a legislated requirement to do so.

Just quickly turning to inquiries where we know that the inquiry was made by an individual. In most of these cases we have an individual who is calling either as an employee of a nonprofit or a donor, a client, or a member of a nonprofit, and usually they have an issue that they're concerned about, that their own personal information has been collected or disclosed, or they want to know how to obtain access to their information. In almost all of these cases we would not have jurisdiction, and we would advise the individual that if they submitted a complaint, we would likely find that there was no jurisdiction, again because there is no commercial activity.

I think some of the topics that they're calling about are or have the potential to be fairly significant privacy issues. There were inquiries about recording conversations, photocopying identification documents, collecting personal employee information, video surveillance by employees, collecting medical information, security clearance checks on prospective employees and volunteers. So those are certainly the same kinds of issues that we see with other commercial organizations that we regulate under PIPA. A lot of the calls from individuals had to do with disclosure of personal information, and again those inquiries generally, surprisingly perhaps, are about photographs and membership lists and things like that although I note that 20 of those had to do with disclosure of personal employee information.

I did also make some inquiries of B.C. OIPC to find out what their experience has been with nonprofits. Nonprofit organizations in British Columbia are fully under the legislation, and what I found out is that B.C. does not track nonprofits because they have no need to. There is no special status for nonprofit organizations under the act, so they don't specifically collect that kind of information. They were able to tell me, though, how many cases they had opened. I would like to note that when B.C. opens a case, they assign a case number to telephone inquiries, written inquiries, e-mail inquiries as well as actual investigations, so that's what is included in their number of approximately 390 cases. They indicated that most of those have to do with church groups, social assistance groups, and minor sports associations. Again, in the inquiries to our office where a specific kind of nonprofit is mentioned, minor sports associations and church groups tend to come up frequently.

B.C. advised me that most of their inquiries are also about general compliance with the act, so looking for assistance in writing a privacy policy or best practices for safeguarding information and also requests for access to information.

The Chair: Thank you. Finally, we're going to be looking at the policy option paper on not-for-profit organizations, scope of the act with respect to not-for-profit organizations. Kim will lead us through that discussion on the first policy option paper.

Ms Lynas: Before we get into that paper, one other thing that I didn't have on the list earlier was that at the last meeting a briefing was requested by the review committee on protection from liability, dealing with volunteers under nonprofits, and I thought we should probably review that before we get into the policy option paper. Amanda is going to present that.

The Chair: We do have some additional copies if members don't have their copy of that piece.

Because this is a walk-on, I'll ask you to be very tight because I think we're about ready to come into the discussion.

Ms Swanek: As we just heard, volunteers are included in the definition of employee in PIPA. PIPA applies in the same way, then, to both volunteers and employees of an organization that is subject to PIPA. In terms of liability this is how PIPA applies. An organization is generally responsible for the actions of its employees and volunteers, and that includes ensuring compliance with PIPA. If an employee or volunteer of an organization contravenes the act, the organization is responsible for the contravention and is liable under the act. The Information and Privacy Commissioner can issue an order finding that an organization has not complied with the act, and where an order has been made, an individual who has suffered a loss or injury because of the organization's violation of the act has a cause of action against the organization for damages.

10:10

Now, the act also provides organizations with protection from legal actions for some breaches of the act. An organization or a person acting on behalf of the organization, such as the employee or volunteer, is protected from legal action for damages resulting from an inappropriate disclosure of personal information if the disclosure was in good faith or failure to provide notice as required under PIPA if reasonable care was taken to give that required notice.

However, where an individual employee or volunteer of an organization has committed an offence under the act, that employee or volunteer may be charged with the offence instead of the organization. Offences are prosecuted by Alberta Justice. Where an employee or volunteer of an organization commits an offence, he or she may be held responsible rather than the organization. It's an offence under the act to wilfully collect, use, or disclose personal information in contravention of the act; wilfully try to or obtain access to personal information in contravention of the act; destroy, hide, or change personal information with an intent to evade an access request; obstruct or knowingly mislead the commissioner or one of his staff; or not follow a commissioner's order.

A person who commits an offence under the act is liable for a fine up to $10,000 for an individual, $100,000 for an organization. These offences only apply to wilful actions by the individual or organization, so the protection from liability for those good-faith actions does not apply. Where an offence has occurred but the court is satisfied that the employee or the volunteer acted reasonably in the circumstances, that employee or volunteer cannot be found guilty of that offence.

So individual employees and volunteers of an organization governed by PIPA can be held personally responsible for a breach of the act but only in limited circumstances. Each of these circumstances requires an intentional act. Even where an individual employee or volunteer performs an action that would otherwise be

an offence under PIPA, that individual cannot be found guilty of the offence if the individual can satisfy the court that he or she acted reasonably in the circumstances.

There are six offences under the act. Most violations of the act do not lead to an offence. For those violations that don't lead to an offence, the organization is responsible for the breach, not the individual volunteer or employee.

The Chair: Thank you.

Mr. VanderBurg: Amanda, you know, under the act you'd have to really do something to get a fine. Has anyone ever been fined the maximum amount?

Ms Swanek: No.

Mr. VanderBurg: Has anyone ever been fined at all?

Ms Swanek: No.

Mr. VanderBurg: Yeah.

The Chair: Laurie.

Ms Blakeman: Yeah. My question was: has anyone been prosecuted? It looks like no. Okay, then: not prosecuted or fined, maximum or minimum.

Mr. VanderBurg: So it's pretty minor. Nobody has wilfully tried to go out there and contravene the act, right?

Ms Swanek: Not as far as we've known.

The Chair: But thank you for bringing that to the table.

Okay. We'll move on to the option paper.

Ms Kreutzer Work: The policy option paper looks at two issues regarding nonprofits. The first deals with the application of PIPA to nonprofits, and that's the main issue. The second issue deals with the narrow question of disclosure of membership lists in very limited, certain circumstances.

I'll start with the first issue. In Alberta there are more than 19,000 not-for-profit organizations, and I use this term to include voluntary and charitable organizations. These organizations are extremely diverse in the services they provide, in the population they serve, the way in which they're formed, the size of their budget, and the number of volunteers, paid staff, clients, and donors.

The two largest categories of not-for-profit organizations are sports and recreation organizations and religious organizations. Other primary areas of activities that not-for-profits participate in include arts and culture and social services. Most organizations serve their local community whether it's a neighbourhood, the city, the town, or the rural municipality. A majority provide the goods or services directly to people, targeting both the general public and various segments of the population such as children, youth, seniors, or persons with disabilities.

Now, during the development of PIPA careful consideration was given to how the act would apply to not-for-profits. It was important that not-for-profits in Alberta be covered at a minimum to the same extent as they would be under the federal private-sector privacy act, PIPEDA. If these organizations were completely excluded from PIPA, they would have by default become subject to the federal act. The government of Alberta chose to limit the application of PIPA to not-for-profits along the same lines as PIPEDA. In other words, not-for-profit organizations as they're defined in the act would have to comply with PIPA only when they collect, use, or disclose personal information in connection with a commercial activity.

Defining a nonprofit organization for purposes of PIPA was a great challenge. First, it had to be simple for organizations to determine whether or not they were a nonprofit for purposes of the act. Second, their status as a nonprofit under the act could not change from year to year. Not only would this be an administrative nightmare if they were in and out on different years, but it would also confuse individuals whether or not they had a right of access to their own personal information or whether they had ability to complain to the commissioner. This, therefore, ruled out any criteria that were fluctuating in nature such as total revenue or number of employees.

Section 56 of PIPA defines a nonprofit organization as this: it is an organization "that is incorporated under the Societies Act or the Agricultural Societies Act or that is registered under Part 9 of the Companies Act." I'll be calling those organizations that fall within that definition of section 56 nonprofits. As was mentioned earlier, section 56 nonprofits are subject to PIPA only when they collect, use, or disclose personal information in connection with a commercial activity. Hilary gave you a brief discussion on commercial activity, so I'm not going to go into any more detail on that.

Now, the act's definition of a nonprofit organization in section 56 has resulted in the act treating similar organizations differently; i.e., not-for-profit organizations that fall within the definition and those that do not. This, in turn, has resulted in the personal information of employees, volunteers, donors, and clients of these similar organizations being treated differently under the act. In the eyes of some of the respondents to the committee's discussion paper this is an issue of fairness.

Let me elaborate on this. Not all not-for-profit organizations are incorporated under the Societies Act, the Agricultural Societies Act, or registered under part 9 of the Companies Act. Some may be established under other public acts of Alberta. For example, some religious congregations are incorporated under the Religious Societies' Land Act, or housing co-operatives are under the Cooperatives Act. Other not-for-profits may be incorporated by a private act of either Alberta or Canada. Others may be incorporated under part 2 of the federal Canada Corporations Act, and still other organizations may just remain as unincorporated associations. So all these organizations do not fall within the act's definition of nonprofit organizations, and therefore they are fully subject to the act as any other business or corporation.

Now, the fact that the act applies in full to some not-for-profit organizations and to others only when they're carrying on a commercial activity has implications for the organization and also for the individuals whose personal information is involved. I'm going to start from the perspective of the individuals. First up will be the clients, the people who receive the services from not-for-profit organizations. Many not-for-profits handle very sensitive personal information about their clients. This is particularly true if they are involved in providing social services or health programs such as emergency shelters, drug or alcohol addiction counselling, financial assistance, living assistance programs for seniors or persons with disabilities.

10:20

Imagine that you are the client. If you are receiving a service from a section 56 nonprofit organization, your personal information is outside the scope of the act unless the program is a commercial

activity. This means that typically the organization is not required to provide you with notice of the purposes for which it is collecting your personal information. You do not have a statutory right to request access to or to correct your personal information held by that organization. The organization does not have to limit the amount of personal information it collects about you for that purpose. The organization does not have to make a reasonable effort to ensure that the information is stored in a secure place such as a locked filing cabinet or ensure that your file is only seen by those members of the staff that have a need to know. In addition, if you don't like the way the organization is handling your personal information, the commissioner cannot investigate your complaint. In contrast, if you as a client were receiving this service from a not-for-profit organization that is fully subject to PIPA, the organization would have those obligations, and you would have those rights that I just mentioned.

Now, what if a section 56 nonprofit operates both commercial and noncommercial activities? Well, in that case different clients could end up being treated differently, or the same client could be even treated differently by one organization. It's going to depend on whether the service is a commercial activity or not. For example, a client who pays for a counselling service is likely to have his personal information protected under the act because that is a commercial activity while the client who receives the service without a fee would not have the same protection in law for his personal information.

One last point about protection of personal information for clients, and I'll call this the chilling effect. Let's say that a government department wants to work with a section 56 nonprofit organization in a program to assist victims of domestic violence. The government department, which is subject to FOIP, is obliged to protect all personal information, so it is very nervous about working with an organization that has no legal obligation to protect that information.

Let's look at the issue from the perspective of paid staff members and volunteers. Say you work or you volunteer for an organization that deals with young children. Because they are involved with young children, they ask you for and you provide a criminal record check. If that organization is a not-for-profit that must comply fully with PIPA, you will have the same rights and protections as if you were an employee of a store or a company. The organization could only use the information it collected for the purpose for which it was collected. The organization would have to make a reasonable effort to ensure that your criminal record check was stored in a secure place, and only those individuals within the organization that had a need to know would have access to that record. But if the organization that you are volunteering for is a section 56 nonprofit, there is no legal obligation for them to protect your information in the same way.

Looking at the issue from the perspective of donors, the personal information of donors typically includes an individual's name, their contact information, the donation amount, and possibly credit card information. Organizations may also compile detailed profiles on selected donors and potential donors for fundraising purposes. Now, a donor of a section 56 nonprofit organization can complain to the commissioner if the organization sells his personal information without consent, because the sale of a membership list is a commercial activity, but the same individual wouldn't have a right to complain if the organization published sensitive personal information about him without consent on its website.

Let's look at the issue from the perspective of organizations. You have two service clubs, both of whom provide similar services to the public. The service club incorporated under the Societies Act does not have the administrative responsibilities of complying with PIPA because it is a section 56 nonprofit. It does not have to comply with PIPA if it is not carrying on a commercial activity. However, a similar service club which is an unincorporated association has the same obligation as any business or other organization under PIPA. Now, if this club were to incorporate under the Societies Act in the future, it would no longer be obliged under PIPA to protect the personal information of its members, its paid staff, its volunteers, or donors.

There is a concern that making section 56 nonprofit organizations subject to PIPA would add to their administrative burden. However, the way the act presently works places its own demands on these organizations. First, they have to grapple with the question of what is a commercial activity. Second, if they carry on both commercial and noncommercial activities, then ostensibly they could have two sets of rules applying to personal information of clients and employees. To resolve the impracticalities of having two sets of rules, some organizations choose to adopt a higher standard of protection and implement a privacy policy for all of their personal information, but doing so would not give the individual a right of access to his or her own personal information or the commissioner the right of review over personal information that is not connected with a commercial activity.

Some section 56 nonprofits that interact with other organizations that are subject to PIPA entirely have adopted their own privacy policy and practices. They see it as an advantage to maintain the same privacy protection for personal information as is required of the other organization.

One last point. PIPA was developed with a view to making informational privacy rules easier for small and medium-sized businesses to understand and implement. If small and medium-sized nonprofit organizations were fully subject to PIPA, their obligations under the act would be the same as those for small and medium-sized businesses. The resources prepared by Service Alberta and the office of the Information and Privacy Commissioner for small and medium-sized businesses would assist nonprofits.

Now, recommendation 13 of the government submission requests that the committee consider the application of the act to nonprofit organizations. Recommendation 1 of the Information and Privacy Commissioner's submission recommends that the coverage of PIPA be extended to all nonprofits in respect of all of their activities. The commissioner suggests that implementation could be delayed one year to allow nonprofits to prepare for compliance.

So the first issue before the committee is whether the act should be amended to change the way it applies to nonprofit organizations. You should have in the handouts that were given to you just this morning a chart that looks like this. We've prepared the chart to help you understand both the policy considerations that I've just gone through as well as the options that I'm going to present in a minute. If you look at the chart, at the bottom of it under the title Policy Considerations the blue section refers to privacy protection. This is probably more of a concern for individuals. The red area, stability from year to year and minimization of regulatory burden, is probably a bigger concern for organizations. In the middle the pink strip, similar treatment under PIPA for similar situations: the issue of fairness is probably a concern for both individuals and organizations.

I just want to point out that one other policy consideration is that the general purpose of the act is to balance the informational rights of the individual with an organization's need to collect, use, and disclose personal information for reasonable purposes.

Now, just above that you have the horizontal line graph, and that shows the spectrum of the protection provided for personal information under the options. At the far left side the minimum standard is set by PIPEDA, where all not-for-profits comply with the act only

when they carry on a commercial activity. At the far right of the side of the scale is maximum coverage for nonprofit organizations. This is where the B.C. PIPA is. As Jill mentioned, in British Columbia all nonprofit organizations are subject to the act, and they have been so since the act came into force in 2004.

There are three options for the committee's consideration, and they're outlined in more detail on page 14 of the policy option paper. The first option is maintaining the status quo. The advantage is that there is a simple, objective means of determining whether an organization is a nonprofit under the act. The main disadvantage is that it doesn't resolve the issue of fairness.

Option 3 moves us to the far right side of the scale. All nonprofits would be fully subject to the act. This provides the maximum, or the highest, level of privacy protection for personal information. This is the position the commissioner has recommended, and it is how nonprofits are treated in B.C. The key advantage is that it resolves the issue of fairness; that is, the different treatment of similar organizations under the act.

The disadvantage is that it increases the administrative burden of those section 56 nonprofit organizations that presently do not have to comply with the act. The commissioner has suggested a one-year transition period. Also, the commissioner said in his oral presentation to the committee that his office would assist nonprofit organizations in learning about the act.

10:30

Option 2 moves to the left side of the scale. It would add additional categories of organizations to section 56. These organizations would only have to comply with PIPA in respect of commercial activities. Personal information in the hands of these organizations would have less privacy protection. There are two suggestions for expanding the category of nonprofit organizations to include other not-for-profits. Option 2(a) is to include religious organizations that are incorporated under a public or private act of Alberta or Canada. The main advantage to this is that it resolves to some extent the issue of similar religious organizations being treated differently under the act, as congregations incorporated by a private act or under the Religious Societies Land Act would now fall under the definition of a nonprofit organization. Some of the disadvantages with 2(a) are the difficulty in defining what is a religious organization and that the privacy protection for personal information under the act is removed for more individuals.

Now, option 2(b) moves us a little more to the left as it would increase the number of organizations that would be defined as a nonprofit organization for purposes of PIPA. These would be the organizations that under the federal Income Tax Act are recognized as nonprofits or are registered as charitable organizations. It resolves to some extent the fairness issue, and it uses an objective criteria. Disadvantages include that it may capture a broader range of organizations than intended. Status as a nonprofit or registered charity can change, and it does remove the privacy protection for a larger number of clients, employees, volunteers, and donors.

The Chair: Thank you.

Okay. We're really kind of at the moment, I suppose, on the not-for-profits for discussion. Are there any questions, first of all, before we begin discussion? No questions.

I see before me three options on this particular question. Option 1 is that we maintain. Option 2 is that we amend the act to talk about "in respect of commercial activities." The final option would make all nonprofit organizations fully subject to PIPA. That is the question before the committee right now. I open the floor for discussion.

Ms Blakeman: I think what we've inadvertently created in the not-for-profit sector – and by that I include charities, volunteer driven, however you want to classify them – is a series of three tests that they were having to experience. They had to determine if they were a not-for-profit under this act, mostly under section 56. Two, they had to determine whether they were engaged in commercial activity. I've been at this for a while, but I found it a struggle to really get a solid definition of what is a commercial activity, and if I'm struggling to find this out and figure it out and had to go to different sources to try and find it – ultimately, in one of your documents it referred to the PIPEDA definition, which I was able to copy out and stick in the front – it's very difficult for groups that don't have the resources that I have as a legislator to try and determine that.

The third test they had to go through was whether it, in fact, applied to everybody they dealt with, and we have determined that third question for them now in including the officials in our last go-round. I think that what they made clear to us when the two groups presented to us, that being the Edmonton Federation of Community Leagues and the Edmonton Chamber of Voluntary Organizations, was that they need certainty, they need clarity, and they need fairness, and I don't think we've achieved that currently.

The last thing is that if we recommend including all nonprofits under PIPA and having PIPA apply to everybody across, what do we gain? Well, one, we do treat everybody the same. You've got a situation right now where the same individual could be treated differently by the same organization depending on whether or not their contact was involving commercial activity. So you could be dealing with an organization in a noncommercial activity portion of what they did and have coverage or not have coverage in one way and then deal with something else that the organization did and be covered a different way, which, frankly, is insanity.

What we need to do is try and achieve some clarity, some certainty, and some fairness here. I recommend that we go with option 3 and have the application of PIPA be to all not-for-profit organizations. I don't think it will be an undue administrative burden to them because increasingly not-for-profits are engaged in commercial activity in some way, shape, or form. As a matter of fact, this very government requires it in many cases to prove that you have some sort of commercial endeavour in order to be eligible for grants, and it's a considerable consideration as to whether you get a grant or not based on your commercial activity.

I think everyone will fall under this eventually, but we might as well do it cleanly. I don't think it will be that much of an administrative burden, especially given the groundwork that's already been done to explain this to the small and medium-size businesses and develop the supporting training sessions and information bulletins to help them understand how to do this.

Coming from the not-for-profit sector, I'm fairly comfortable that this is an achievable thing for groups to do. There will be a learning curve. We need to give them time to come into it, as recommended by the Privacy Commissioner, but I think this is the way we have to do it because right now it's an unbelievable hodgepodge.

The Chair: Ms Blakeman, did you want to move option 3?

Ms Blakeman: Yes, I will move option 3. I don't have the wording in front of me anymore.

The Chair: That the Select Special Personal Information Protection Act Review Committee recommend that the act be amended to make all nonprofit organizations fully subject to PIPA.

Ms Blakeman: Yes, indeed. That's exactly what I said.

Mr. VanderBurg: With the one-year provision?

Ms Blakeman: Yes. Can we put in the one year, that it would be phased in over a year, that it would be phased in after a year of training?

The Chair: Okay. We'll add that to the amendment. Any questions?

Mr. Martin: Well, I'm certainly going to support it. I think the KISS principle is important: keep it simple, stupid. I wouldn't begin to even try to understand who qualified under the way we have it now, so if it's working in B.C., I think it makes some sense.

There'll be some nervousness out there by smaller groups. You know, we can talk about the soccer clubs and those sorts of things. What makes me a little more comfortable is the previous discussion about liability. I think that information should get out, that you have to wilfully do something before you're going to be held liable. I think that's a concern with some of these smaller groups.

I think it's also important – and we have to say this to the Privacy Commissioner – that with that year there be that information that he was talking about. Give people time; get that information out to them. That's not going to be that complicated. Things aren't going to change that much if you're a small organization. That's extremely important. Otherwise, there's going to be a lot of anxiety, if I can put it that way. I think the information that he sends out and the ability for them to ask questions, those sorts of things, are very important.

Just on the previous discussion, I mean, it's just far too complicated, and I think this makes it simple, straightforward if all the other things are done in the year, with the giving of information. So I'd certainly support it.

The Chair: Any other members? No? Laurie, one more?

Ms Blakeman: Just the last thing for anyone that gets around to reading the *Hansard* for this. I think what's important to remember and what we often get away from is that for these not-for-profit organizations the information we're talking about is personal information. It's not about how the organization works or its bylaws. Those are subject to other things. We're talking about the protection of people's personal information that the organization has collected, and we need to encourage organizations to only collect what they need and only use it for what they collected it for. Those are the two primary points. Once we all are on the same track there, this will be a lot easier.

10:40

Mr. Lund: Well, I only have one question to the staff, and that would be: if an organization has a membership and they would like to disclose that membership to other members in their organization, could they do this simply by a motion of the organization that's passed?

Ms Kreutzer Work: This is an issue that we're going to approach next in the policy option paper. There are some acts that allow certain nonprofit organizations to disclose a membership list to their members for that member to use for matters relating to the affairs of the organization, and because PIPA says that if an act or a regulation authorizes disclosure of personal information, the organization can disclose the information without consent. So it would depend on how the organization had the ability in its own legislation to disclose the information.

Mr. Lund: If I could just elaborate a little bit. When we passed FOIP, things like the picture of the graduates of a high school in a paper was deemed to be against FOIP unless there was written consent of the individual. In the Rocky constituency that caused huge, huge concern. People thought we'd gone way overboard.

Another thing that I know happens – and I'm sure it happens in all of the rural papers – is that when there are different bonspiels, for example, the list of the individuals that are on the teams is published in the local paper. I would hate to think that somehow the organizers have to get permission from every individual that is going to be in that bonspiel. As a matter of fact, the time schedule and who plays who are in there, so those names are in there again. Can they do that without acting against this act?

Ms Lynas: They would need consent. Now, there are the different forms of consent, including consent that can be given orally. Typically, what organizations would need to do is at the time the person signs up for the league and is paying their fee and giving their phone number so they can be contacted to organize games and that sort of thing, the organization would tell them: we will give our lists to the newspapers. That would cover it because the individual would sign a consent for all the purposes up front.

Now, when the local newspaper goes out to cover it, they're under that exclusion for journalistic purposes, so they don't need consent to take a photograph of the teams and publish it in the papers or when they go and interview team members, write up stories. They don't need that consent for the publicity. The organization would handle its own publicity consent by advising the players how their personal information would be used – we give it to our Alberta organization; we publicize events; we give it to visiting teams, that kind of thing, whatever they do – getting a general consent at the beginning of the year and being done with it.

Ms Blakeman: Would 14(f) cover that: "is necessary to determine the individual's suitability to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary"?

Ms Lynas: I wouldn't think so.

Ms Blakeman: Okay.

The Chair: Okay. Are there any more questions by the committee before I call this question? Seeing none, I will ask if the committee is in favour of the motion as moved by member Laurie Blakeman. I don't think I need to read it; it's already been read into the record. All of you have it in front of you. Would you like me to repeat it? That

> the Select Special Personal Information Protection Act Review Committee recommend that the act be amended to make all not-for-profit organizations fully subject to PIPA, to be phased in over a one-year period.

All those members in favour? Any opposed? Ty Lund is opposed, for the record. Thank you. So it is carried.

We're going to now move on to the membership list disclosure. It's another portion of this question. We have two options in front of us: one is to maintain the status quo, and the other is to amend the act. I'll let them go ahead and do the update before we look at this question further.

Go ahead.

Ms Kreutzer Work: Just a little background information. David Jones, when he was acting on behalf of the Anglican Diocese of Edmonton, stated in his oral presentation to the committee that all churches should have the ability to disclose without consent a list of

congregation members for use by a member for matters relating to the affairs of the congregation.

At present the congregations incorporated under the Religious Societies' Land Act and the Societies Act can disclose a membership list for this limited purpose. Those statutes contain a special provision permitting such disclosure, and, as I said earlier, PIPA says that if an act or regulation authorizes a disclosure of personal information, the organization can disclose that personal information without consent. As we know from our earlier discussion, not all religious organizations are incorporated under the Religious Societies' Land Act or the Societies Act. Congregations that are not incorporated under those acts may not have the same ability to disclose the membership list for that limited purpose.

Now, if congregations were to be given this limited ability to disclose the membership list without consent for use by a member for matters relating to the affairs of the congregation, this would be an amendment to PIPA. It would not be an amendment to the Religious Societies' Land Act or the Societies Act. So the issue for the committee's consideration is whether PIPA should be amended to allow religious organizations to disclose a membership list for use by a member for matters relating to the affairs of the congregation.

The first option is maintaining the status quo. A couple of points. It is unclear whether every religious organization maintains a membership list. Some congregations do have very formal membership lists and others not so much. It is also uncertain why obtaining consent would be problematic. The advantage to maintaining the status quo is that it maintains the general PIPA principle that personal information be disclosed only with consent. The disadvantage is that different rules will apply to religious organizations depending on how that organization is established.

Now, the second option would allow each religious organization to decide for itself whether its membership lists should be disclosed without consent for this purpose. This option would require an amendment to the act that would create a new exception to consent for the disclosure of the membership list. Exception to consent, just as a reminder, means that an individual does not have the ability to withdraw consent for this disclosure because there was no consent in the first place. In order to use the exception to consent in PIPA, if it was created, there would be certain preconditions. First, the organization would have to have some power under an act or regulation to enact bylaw resolution rules or some other form of legislative instrument to carry out administrative functions. Second, if an organization decides that it needs to disclose its membership list without consent for this purpose, it must formalize that decision by enacting such a bylaw resolution or whatever. This allows for transparency and accountability about the disclosure of members' personal information within the congregation.

The advantages of option 2: it resolves the issue of incorporated religious organizations being treated differently with respect to disclosure of membership lists for this purpose, and, as I mentioned, it provides transparency and accountability regarding the disclosure of the list. Disadvantages: two key disadvantages are that it expands the act's exceptions to consent and the difficulty in defining what is a religious organization.

The Chair: It's always been difficult to determine what is the definition of a religious organization, except for the one I belong to, of course.

Anyway, that is not the nature of the question. The question is, as you have before you, two options on the disclosure of membership lists to other members. Are there any questions before we look to see if there's a motion from the floor? Any questions from the committee?

Ms Blakeman: I'm sorry. Was there a recommendation from the Privacy Commissioner or from Service Alberta on this?

Ms Kreutzer Work: No.

Ms Blakeman: Okay. Thanks.

10:50

The Chair: Would anyone like to move the amendment, or are we in favour? Well, I guess I could bring forward option 1 if there is no motion from the floor.

Would the members like to maintain the status quo?

I'll call that question. All those in favour? Those opposed? Did all members vote?

Okay. As you know from last week, we have a standing order that says that all members must vote or it's off with your head. Obviously there's still some need for clarification. Are you feeling some discomfort with the question?

Mr. Webber: I'm just looking at the question here. Just give me 30 seconds.

The Chair: Okay.

Ms Blakeman: Would option 2 have addressed the concerns that were raised by was it David Jones from the Anglican diocese?

Ms Kreutzer Work: I think largely it would address his concern that all religious organizations have the same ability to disclose their membership list. The one little bit that it may not cover was that if there was a religious organization that was not established under some act that gave it a power to enact a bylaw or a resolution or a regulation, we'd want a legislative instrument of that organization in order to be able to disclose it without consent under PIPA. It's the same way that we treat professional regulatory organizations under PIPA.

Ms Blakeman: Oh. Right. Now, what about – I'm trying to choose my words carefully here – if I started a church called Everybody Must Live Here, and it had some really interesting practices that were questionable by other people's definitions. Would this apply to it?

Ms Kreutzer Work: I guess it depends on how it would be established. You just created this in your own neighbourhood kind of thing.

Ms Blakeman: It's the church of Laurie. Yes.

Ms Kreutzer Work: I think you'd have a hard time meeting the requirement that you have a legislative instrument to enact a bylaw that would be classified as a regulation under PIPA, and therefore it would allow for the disclosure without consent.

Ms Blakeman: But any church that captured itself under the Societies Act or got itself through as a private member's private bill . . .

Ms Kreutzer Work: Yes. Whether it's Alberta or federal.

The Chair: So, Ray, we're hoping you're not going to start a church, but you're up next.

Mr. Martin: No.

The Chair: You're not planning on it?

Mr. Martin: I could only get Len Webber to join.

Ms Blakeman: And he's thinking about it.

Mr. Martin: Yeah. He's thinking about it.

No. I think we have to be cautious here. I understand that it's there, you know, the purpose, but it's assuming that even within a religious organization everybody thinks the same. In the Anglican church they've just had a major debate about a very contentious issue, and I think there's a potential somewhat for abuse in different organizations with the membership list. As I said, I think it's moving away somewhat from the spirit of PIPA, and I think we'd be opening up a can of worms here. I certainly think that we should stay with the status quo.

Mr. Ducharme: Speaking to the status quo, when I look at the reason that we've stated it as a disadvantage, I believe the flexibility is there for any religious organization to solve their own issue themselves without us having to legislate it, and that's why I favour the status quo option.

The Chair: Okay. I am going to call the question again.

Mr. Webber: Do we have to?

The Chair: You have no option. You must vote one way or the other. Unless you have a question you'd like to ask before I call it.

Mr. Webber: Well, you can call it again. I just thought that it was called, and it was just up to me to decide where I wanted to vote.

The Chair: Oh, legally, yeah, you're right. I already have everyone else on the record, so I guess we are looking to you, hon. member.

Mr. Webber: I would vote to maintain the status quo.

The Chair: Okay. Then that carries: option 1, to maintain the status quo.

Okay. I'm going to call just a short break. We have an administrative issue, so if you want to run to the bathroom, grab something to drink, you've got five minutes, please, and then we'll continue.

[The committee adjourned from 10:55 a.m. to 11:07 a.m.]

[Mr. VanderBurg in the chair]

The Deputy Chair: Okay. Everybody is re-energized, and we're ready to go. We'll go on to item 6. Hilary, for a brief explanation.

Ms Lynas: Okay. The next question is about professional regulatory organizations. So we're talking about self-governing professional or occupational bodies that are incorporated under a statute that provides for regulation. An example is the Law Society or the Institute of Chartered Accountants of Alberta, and a occupational association is something like the Association of School Business Officials of Alberta. Because of their need to balance the protection of personal information with a government mandate to protect the public interest in regulating the profession, there are some special provisions built into PIPA.

A professional regulatory organization may develop a personal information code. What they can do is write up their own code. It has to provide the same level of privacy protection as in the act, but they can use their own terminology or refer to their own committees, bylaws, et cetera, as necessary within the code. As of June this year we don't have any personal information codes in place for professional regulatory associations. It's a provision in the act that's available to professional regulatory organizations, but it hasn't been used yet.

In terms of the comments that were received, there were some around the disciplinary process of a PRO. Four organizations stated that delays in disciplinary process due to parallel proceedings under the PRO's governing legislation and under PIPA should be discouraged. They are still required to process requests for access made under PIPA. Professional regulatory organizations generally have their own rules on access to information for the purpose of disciplinary proceedings. The process for obtaining access under PIPA is separate from other processes and doesn't override an organization's legislation regarding access for a proceeding.

Regarding personal information codes, five organizations recommended that PIPA be amended to allow organizations to adopt personal information codes that comply with the organization's disclosure obligations pursuant to common law and their own governing legislation and that receive approval by the commissioner even though they don't strictly comply with PIPA. One individual suggested that professional regulatory organizations be required to develop a personal information code as they provide some assurance that the act will be applied in a fair and consistent manner.

Five professional regulatory organizations questioned keeping the provision for personal information codes if none have been developed to date. We do have an issue paper on personal information codes that we're going to discuss in just a moment.

One professional regulatory organization suggested that membership data required by trade union or professional associations should be added as an exception to consent, but we note that PIPA permits the collection of personal information without consent of the individual if it's necessary to comply with a collective agreement under the labour relations code.

The Deputy Chair: Then we have issue paper 5. Jann, do you want to briefly cover that before we decide whether we should do anything or not with this?

Ms Lynn-George: Okay. I would emphasize that among *Hansard* readers you'll probably find a lot of these professional regulatory organizations, or PROs, as I'll call them to be brief. They have followed this issue from the beginning. They have been extensively involved in consultation, and they have very strong views on some of their issues.

During the development of PIPA PROs were really concerned that being subject to PIPA might interfere with their ability to act in the public interest, which they considered to set them apart from other organizations that are subject to this act. They're worried that the act might limit their ability to conduct investigations and disciplinary proceedings effectively and to inform the public about members who have been disciplined. They were concerned about requests for access during the process. They didn't want parallel proceedings, and they didn't want to have individuals going to the commissioner at the same time as the matter was under consideration by one of their committees.

The act was intended to address these issues, and the commissioner has endorsed the approach that's been taken and said very clearly that these different statutes, the professional acts and PIPA, are quite separate even though in some cases they may be complementary. So he didn't feel that PIPA was problematic for the operation of this professional legislation.

How does PIPA apply to PROs? Well, a PRO can collect, use, and disclose personal information with consent or without consent if the act provides for that. There's one no consent provision that's particularly important for PROs, and that's where the act says that an organization can collect, use, or disclose if a statute or regulation says that they can. PIPA specifically says – and it makes an exception for PROs – that if the PRO establishes a rule or bylaw saying that there can be some collection, use, or disclosure without consent, then that's okay under PIPA as well. That's an exceptional provision.

Ms Blakeman: Where is that?

Ms Lynn-George: It's in the definition of statute or regulation in the regulation.

Then, the other thing that's very important in the act is that it says that an organization can collect, use, or disclose for the purpose of an investigation or a legal proceeding, and those definitions were developed to make sure that they apply to every stage of the process in a disciplinary hearing by a PRO. A PRO can also refuse to provide access to personal information that was collected for an investigation or legal proceeding. The act does not have any harm's test. It's entirely at the discretion of the organization to decide what it will or won't disclose, so quite a permissive provision among those in the access section of the act.

11:15

Now, if the Information and Privacy Commissioner receives a complaint or a request for a review, there's another provision in the act that is helpful to PROs because the act says that if there is another grievance, complaint, or review procedure that can be used to resolve the issues, then the commissioner can send that individual back and say that the individual has to exhaust those procedures first. The idea is to encourage individuals to handle all their issues in one forum.

So that's the way the act applies in general, but there's this other provision in the act, and this is special for PROs. It says that a PRO can establish a personal information code. The organizations themselves were very supportive of this concept, and it was expected that the code could have some advantages for them. It could be a simplified version of the principles set out in the act that could be made directly relevant and meaningful to the profession, its members, and the public. A code could be developed to harmonize with other elements of a PRO's governing legislation, including its own rules. It could all be a single package. A PRO with a code could use an existing internal complaint-handling process for all its privacy complaints. So those were the advantages.

But there were also some disadvantages. First of all, a code has to be developed, implemented, and it has to be kept up to date. There are costs. A code also provides less certainty for members and the public, at least in the initial stages. Thirdly, it just might not be worth the effort. It might just be simpler to comply with the act and develop some policies and procedures to explain the way it all works.

Our branch has published a guide and a model code on our website since 2003. The branch has been consulted on some drafts, but so far no PRO has come to the point of asking the minister to authorize a code.

So we've got an issue here. PROs deal with highly sensitive information in circumstances where individuals have a high level of personal investment in the decisions. Decisions of a PRO can affect an individual's reputation and livelihood. Several PROs have said that the provision for a personal information code is ineffective. Some PROs are interested in retaining the code provisions, but they'd like to see the provisions more responsive to the needs of PROs. There's no consensus, however, on how these code provisions could be developed to address their concerns.

So we're putting two options before the committee today. The first is to retain the provisions for personal information codes and revisit the issue during the next review. The main advantage is that the existing provisions may allow for some flexibility. The main disadvantage is that this provision for separate codes may be a little confusing to the public.

The second option is simply to delete the provisions for these personal information codes. The advantage: simplification. The disadvantage: it may be premature at this stage to decide that PROs might not benefit from the flexibility that's offered by this particular provision in the act.

The Deputy Chair: Thanks, Jann.

Denis, do you have a question for Jann?

Mr. Ducharme: No. I'd like to make a motion if I can, Mr. Chair. That's to go with option 1. That's to

> retain the provisions for personal information codes and revisit the issue during the next review of PIPA.

As we just heard from the explanation that's been provide to us, I guess the act is in its infancy. There's still a little bit of discussion that's taking place within the PROs. We may as well leave it there, and then for the next review of PIPA if things haven't changed, well, then we can say, "Well, it's not needed," if there have been no personal codes that have been brought forward by any of them. That's why I'm supportive of option 1.

The Deputy Chair: Hilary explained the flexibility of that option.

Ms Blakeman: My only concern around this is that we only had three individuals present a submission, either written or oral, in some cases both, to the committee, and all of them were about professional regulatory organizations and their extreme unhappiness with their experience there. I have no wish to get involved in individual cases here, but I do note that we only had three individuals, and all of them were concerned about how they were treated and their access to information and the limitations that were placed on them around that. So I would say that this system is not perfect. I'm assuming that those three people represent a lot more that are very unhappy, but it's also worth noting that we didn't hear from hundreds of them; we heard from three.

I'm quite honestly not sure about which way to go with this because I find that we tend to legislate in favour of the larger bodies, which are easier for us to deal with, rather than in favour of individual members of the public, which are less easy to deal with. I'm a little worried that we're tipping the balance here, but I honestly feel that I don't have enough information.

Ms Lynn-George: A piece of this paper that I just chopped was about the submission that came in last week. Were you including that in your three?

Ms Blakeman: Yes, I was.

Ms Lynn-George: Okay. That submission was about a complaint process, and it was her view that PROs should use the personal information codes allowed under PIPA to integrate a higher level of privacy protection into their disciplinary processes. That was just the last item.

The Deputy Chair: We have a motion on the floor, moved by Denis Ducharme: option 1.

Ms Blakeman: And that was to maintain the status quo, correct?

The Deputy Chair: Yes.

All those in favour? All those opposed? It's carried.

We'll move on to the next issue: harmonization.

Ray, just so you know, we don't require any motions. I know you had another appointment that you had to get to. This issue will strictly be a matter of information.

Mr. Martin: I have quite a bit of time yet. I have till 12.

The Deputy Chair: Okay. I just wanted you to know that we're not going to have to have any motions out of this.

Hilary, can you go through the summary of responses?

Ms Lynas: In this question there isn't a page called What PIPA Says because PIPA doesn't say anything about harmonization. The question was added in the discussion guide to find out whether there were any specific amendments needed in PIPA to make it easier for businesses that are operating in Alberta, B.C., and areas under federal jurisdictions. It was important to find out whether there was something that could be redrafted just to make it easier for businesses.

Overall, there didn't seem to be any submissions along that line. Generally there was support for harmonization and ensuring that legislative amendments foster uniformity and consistency of provincial and federal legislation.

One association suggested that if disclosure between two or more substantially similar jurisdictions is in compliance with respective privacy legislation, then compliance with PIPEDA should not be necessary, and one professional regulatory organization stated that it had reviewed PIPEDA and other privacy legislation and policies and found that the PIPA provisions applying to professional regulatory associations were superior to and more understandable than those in PIPEDA.

I'll turn it over to Jann.

11:25

The Deputy Chair: Thank you.

Ms Lynn-George: Amanda is just going to provide some visual aids. While she's doing that, I'd just like to remind you that early in the review process the Deputy Minister of Service Alberta made a presentation to the committee in which he emphasized two issues: the first was nonprofits; the second was harmonization. It was the subject of a government recommendation. This recommendation was a recommendation to the committee, and it was that the committee consider all proposals for amendment in the context of the need to maintain similarity with other private-sector privacy legislation. So there's no motion that would arise from that, but it was a recommendation to the committee.

This briefing on harmonization provides a high-level overview of the issue, but since it maybe all seems rather abstract, we've also provided a map. This may help the committee to visualize harmonization as an issue for organizations. You have before you a map of Canada showing the provincial privacy legislation that applies in each jurisdiction and listing the commissioners or their equivalents that are responsible for oversight. The two federal privacy statutes also apply to federal government institutions and to federally regulated organizations across the country. As you can see, all provinces have public-sector legislation, four have health information legislation, and three have private-sector legislation. PIPEDA applies where there's no provincial private-sector act.

Although all the acts are based on common principles, there are differences. Wherever organizations are subject to more than one act, it's obviously important to them that there are some consistent rules. This is certainly the case where an organization is subject to both PIPA and PIPEDA. Because there are differences between these two acts – for example, PIPA has an exemption to consent for sale of a business which PIPEDA doesn't – it's also important to organizations to know which act applies in a specific situation. This will determine which commissioner has jurisdiction if there's a complaint. Surprisingly, perhaps, this is more difficult with privacy legislation than with a lot of other legislation. It's because of this point that one organization may be disclosing personal information in one jurisdiction and another organization is collecting in another jurisdiction. So that's why the jurisdictional issues arise.

The committee's discussion paper invited respondents to suggest any amendments that would make it easier for them to operate under the three acts: Alberta, B.C., and the federal act. I'll just mention that other jurisdictions are asking the same questions. At the federal level the report on PIPEDA was issued in May this year, and there is a special committee of the B.C. Legislative Assembly appointed on April 19 that will submit a report in the next year.

What we're hearing in Alberta is broad support for harmonization. At the same time, some respondents have expressed a preference for provisions in Alberta PIPA that differ from PIPEDA or B.C. PIPA, such as the exception I mentioned, the sale of a business. So they want harmonization – they want everything to be the same – but they want to keep the elements of the Alberta act that they perceive to be new and improved.

Some organizations are clearly very concerned about the jurisdictional issues. I mention that the main objective of the various recommendations is to clarify the application of PIPA with respect to intraprovincial transactions. Their voices have not gone unheard. Alberta's Information and Privacy Commissioner has developed a publication in collaboration with the B.C. commissioner and the federal Privacy Commissioner to provide practical advice on how organizations that operate in multiple jurisdictions can comply with all three acts.

At this point there does not appear to be a strong case for amending the act. Three points: the select special committee has addressed the issue of harmonization in relation to specific issues and recommendations for amendments to PIPA, second, the committee will also have an opportunity to comment on the significance of harmonization in its final report, and third, Service Alberta will continue to monitor amendments to legislation in other jurisdictions with a view to maintaining similarity to other privacy legislation and promoting harmonization.

The Deputy Chair: Thank you.

Any clarification? We'll move on to item 8, question 10, summary.

Ms Lynas: This is another topic where there is no requirement in the act at the moment. The question was: "should consent be required to send personal information outside of Canada?" This became an issue nationally as a result of a B.C. court challenge where B.C. was proposing to outsource some management of the health care system to a company in the United States, and they were challenged by the union in terms of whether privacy and security would be protected.

Once personal information is transferred outside of Canada, the laws of the country to which the information has been transferred

will apply. These laws will determine whether government agencies, such as law enforcement and tax authorities, can obtain access to personal information. The federal Privacy Commissioner has taken the position that a company in Canada that outsources information processing to the U.S. should notify its customers that the information may be available to the U.S. government or its agencies under a lawful order made in that country. That's why the issue was part of the discussion paper.

The responses are summarized in two categories. One is whether there's a belief that there should be consent to send information outside of Canada, and the other question is whether there should be notice for the same purpose. In terms of consent there is an organization and an individual that suggested that organizations should be required to obtain consent to send personal information outside of Canada. Another business suggested requiring consent only for transmission to an unrelated entity so that international companies could continue to operate without artificial impediments to business enterprising.

Another business said that if a clear statement of notice were given, then separate consent to send the information out of Canada should not be required. Another association noted that allowing individuals to opt out was not really an option and suggested that instead an organization's privacy policy could contain information about its approaches and practices with respect to outsourcing.

Numerous organizations said that consent should not be required, saying that it would be impractical, costly, onerous, or not meaningful to obtain consent every time personal information was sent outside of the country.

In terms of notice and whether it should be required, one professional regulatory organization commented that notice should be mandatory. Others stressed the importance if there was a possible risk of scrutiny of information by non-Canadian governments.

Two businesses suggested that a better approach would be to require adequate contractual provisions for personal information of Albertans that are in any outsourcing contract, keeping in mind the requirements of the laws of the other country involved. PIPEDA does require that organizations that use contractual or other means to provide service are required to provide a comparable level of privacy protection when it is being processed by a third party, regardless of where that's being done.

Other organizations said that notice should not be required, stating that PIPA provides adequate protection and other resources to provide guidance needed for organizations to protect personal information when it's transferred across border. Others said that notification requirements would be onerous and would have a minimal value in ensuring protection of personal information. That's about it.

11:35

The Deputy Chair: Amanda, do you want to comment on the issue paper? Or Jann?

Ms Lynn-George: Okay. This is a somewhat more complex issue. It's about what happens to personal information when it leaves Canada, and I'd like to just present three brief scenarios. The first Hilary has already mentioned, and that's the impact of the USA PATRIOT Act. Concerns have been raised that U.S. service providers might disclose personal information about Canadians to U.S. law enforcement authorities without the agreement or even the knowledge of the parties in Canada for whom they're providing services. That's the essence of the issue, and it was the reason why the Alberta FOIP Act was amended last year. Some considerations are the same for the private sector.

The second case Hilary also mentioned, and that was about the CIBC. In 2004 CIBC Visa updated its cardholder agreement to inform customers that their personal information was being transferred to a U.S. service provider for processing. The cardholder agreement said that the personal information might be accessed by U.S. governments, courts, or law enforcement. As a result, there were many complaints to the federal Privacy Commissioner.

Now, the commissioner investigated the complaints, and as Hilary explained, she found that CIBC had not contravened the federal privacy act. She said that consent for primary use included consent for outsourcing as long as the outsourcing was directly related to the primary purpose of the collection. She also said that an organization has no obligation to obtain consent or to provide clients with the ability to opt out of having their personal information transferred to the service provider. An organization must, however, give notice when it transfers the personal information to the third party. Also, the organization has a duty to protect the personal information by contractual measures. Remember now, that's under PIPEDA, where there's a specific provision for contracts.

My last story is about a case in India. In 2005 a call centre worker in India sold bank account details of 1,000 U.K. customers to an undercover reporter. The reporter was able to buy bank account, credit card, passport, and driver's licence details of U.K. bank customers for less than $10 each. The worker also told the reporter that he could supply confidential data from 200,000 accounts per month. The London police couldn't prosecute, so the matter had to be handled by the Indian authorities. Since India had no privacy protection statute, the matter would have to be prosecuted under other laws. The commissioner responsible for the U.K. privacy act warned U.K. based companies that they are legally liable for any security failings.

None of these were Alberta cases, so why do they matter here? Organizations in Alberta operate within what is increasingly a global business environment. Organizations regularly contract with businesses in other countries for services involving personal information of clients and employees. For example, many organizations outsource payroll services and benefit programs. It's also common for organizations to outsource customer service operations and market research to businesses that operate call centres in other jurisdictions. In addition, there's a growing trend towards the use of foreign service providers for information management services, so a lot of professional corporations store their business records in another jurisdiction.

There are also a lot of businesses that use service providers in other jurisdictions for security purposes, for their off-site backup. This is not uncommon; it's a very ordinary business practice in Alberta today.

So the issue. It's been suggested that Alberta's PIPA may not provide adequate protection for personal information when an organization transfers to a third party for processing or storage outside Alberta. It's been proposed that organizations should be required either to obtain consent or to notify the individual that personal information may be transferred outside the country.

Before we consider the options, let's see how PIPA protects personal information transferred to service providers. Well, first of all, it does so by making the principal organization responsible for the actions of its contractors. Second, it requires organizations to develop policies and practices, so those policies and practices have to be available to individuals on request. Thirdly, when organizations obtain consent, which they normally have to do, they have to provide some notification of the purpose of the collection and somebody who can answer questions about it, so if they have concerns, there is a contact person. Also, there is the general

provision for security, and organizations are responsible under the act for security. There are some questions about how these specific provisions would apply if there were a case involving transfer of personal information to a third party.

I'd like to just talk briefly about each of the proposals here – the first is consent; the second is notification – and some of the implications. First on consent. Consent is the guiding principle in PIPA. The main argument in favour of a consent requirement for outsourcing is that it would enable an individual to decide whether he or she was willing to accept the risk of having his or her personal information transferred to a jurisdiction without protection for personal information that's comparable to what we have in Canada. A consent requirement would not create a duty on the part of organizations to offer an alternative to outsourcing. That's important.

An organization might choose to offer an alternative as a competitive strategy, and you may have seen the ads on television for the U.S. lender E-Loan. It's embraced privacy as a business value and allows the client to choose to have an application processed in the U.S. rather than in Asia. That's a business choice. It's not required under the act to provide an alternative to outsourcing.

The arguments against a consent requirement that were put forward in the responses to the discussion paper are that it's not necessary, that it would be impractical. Many of the respondents felt that PIPA already had strong protection for personal information in the custody of contractors.

A number of the respondents talked about alternative measures. They suggested a due diligence process of selecting a service provider, a risk management process for outsourcing arrangements, adequate contractual protections, and finally, transparency in providing information about an organization's practices. It's notable that of all these measures only the last actually makes information available to the affected individuals, enabling the individual to make the decision to have control over his or her personal information.

There's another consideration that may also be significant. The act normally requires consent for the collection of personal information for a particular purpose. When an organization provides notice of the purposes for which information will be used, it's reasonable to expect that the organization will provide information of significance to the individual.

What do we want to know when an organization takes our personal information? Well, we want to know if it's going to be used to make a decision about an individual, we want to know if it's going to be used for further interaction, and we want to know if it's going to be disclosed to a third party. What we mostly are not so interested in is the standard internal business processes that it's going to be used for. So the question arises when you're talking about outsourcing: is this a practice that is so different from other internal business processes that it really needs to be brought to the attention of an individual and made the subject of consent? That's consent.

11:45

Notification. The main argument in favour of a notification requirement is similar to what it is for consent, that it enables individuals to assess their own risk and make that decision about whether they want to enter into a relationship with that organization. In practical terms there'll be very little difference between consent and notification in a situation involving outsourcing because, as I said before, there's no ability to opt out. So if you don't like it, you go elsewhere. You get the notification, and you have the choice.

The main arguments against a notification requirement are much the same as for consent but a little less so: that PIPA already provides adequate protection and that there are alternative measures. A different line of argument is that the act already requires notice; the commissioner just hasn't had an opportunity to say so yet.

A final consideration. If there's a notification requirement in this instance, the question arises whether there should be an express notification requirement in other instances. That's something that would have to have some attention, whether you might do something unintended if you decided to specify one set of circumstances in which you require notification.

So we've given you four options, and these move down the scale in terms of the requirements on organizations. Starting at the top we have the consent option: provides the highest standard of privacy protection. That's the advantage. The disadvantage is that it has very little support in the business community and may be considered an unreasonable burden on business.

Moving down the scale: the notice option. The advantage: it would be consistent with the principle of allowing individuals the right to control the way their personal information is used. It would also provide clarity. At the moment there is some expectation that notice may already be required. This would provide some certainty. The disadvantage is the same as consent to a somewhat lesser extent: a burden on business.

Third, maintain the status quo. The argument is really that PIPA already provides a lot of protection for personal information that's transferred outside Canada for processing or storage. Main advantage: broader support within the business community than a legislated notification requirement. Disadvantage: this is a big issue, and this might seem to be an inadequate response to a trend that is exposing increasing amounts of personal information to very high risk of exposure.

Fourth, no amendment; try an alternative strategy. This amendment suggests that some guidelines might be developed to improve the quality of protection when businesses are contracting with service providers outside Canada. Advantage: it does address the issue highlighted by organizations that they're the ones who are responsible for protecting personal information. They're the ones who are going to be on the chopping block if something goes wrong. The disadvantage is that it doesn't address the specific issue of putting the decision in the hands of the individual, and ultimately that's what privacy protection is about.

The Deputy Chair: Thanks, Jann.

I have three on the list: Ray, followed by Len, followed by Gord.

Mr. Martin: This has the potential to be one of the most serious things that we deal with, and it seems to me logical that the federal act, whatever its action is, should have been dealing with that because very few of these companies are going to be locally Alberta based. You know, it would probably make more sense to be dealing with it at the national level. CIBC would be an example.

If this ever would have somewhere – I was going to say the PATRIOT Act, but it's not the United States. It's all over the world that outsourcing is going on – you mentioned about the Indian company – so I think we should probably do what we can. I mean, it seems to me that it should be federal. At the very least we should be telling them that they should be doing something about it. That's one recommendation we could make. I would see the need.

I'm not sure, and I'd be easy about the consent because most people probably don't care unless something happens. But the notification: it seems to me that if all of a sudden there's outsourcing to the United States, at least as an individual I may say that I don't want that to happen. I can at least then go to the bank, if it's CIBC as it was in this case, and say, "Well, I'm going to go over to the

Bank of Nova Scotia" or whatever. You know, I have that choice to make if there's a notification. As I say, I'm not sure consent is needed in that regard, but I think a notification is. I think this is a serious matter, when it's shipped out. I'm not sure I want to make a recommendation at this point, but that would be what I would lean towards.

The Deputy Chair: I agree. Probably the status quo is not the option; I agree with you, Ray.

Mr. Webber: A little bit of confusion here with respect to your document on the public consultation, page 6. You've got some numbers here that I think are twisted around. You've got your no comments at 54 per cent, organizations should be required to provide notice at 16 per cent, and organizations should not be required to provide notice at 30 per cent. Then below that you've got the opposite, unless I'm reading it incorrectly, but it says: "Nearly twice as many respondents stated that organizations should be required to provide notice (30%) as stated that providing notice should not be a requirement for organizations (16%)." So I'm just confused. What would be the right figures?

Ms Lynas: I think the table would be the right figures.

Mr. Webber: The table. Thanks.

The Deputy Chair: Thank you.

Mr. Graydon: Some clarification around personal options under the notify individuals option: if you receive a letter from your employer saying, "Effective January 1 we're outsourcing our payroll to Citibank U.S.A.," what are my options?

The Deputy Chair: Who wants to answer that?

Ms Lynn-George: Well, you're talking about if you're an employee?

Mr. Graydon: An employee, yeah, in this case.

Ms Lynn-George: You have no options, but you do know about it if you've received notification.

The Deputy Chair: Okay, Gord?

Mr. Graydon: Yeah. Not the answer I was hoping to hear.

The Deputy Chair: Laurie, followed by Ty.

Ms Blakeman: Thanks very much. To a certain extent I think the horse has left the barn on this one, but I agree with Ray that we should do what we can because if we can't try and protect our citizens and their personal information, who can? I think the issue is one of risk of the personal information. I don't think anybody cares if Citibank U.S.A. has their information if the likelihood that it would get used for a purpose they didn't agree to was very low. People are worried about the information being used for something they didn't want it used for, and I would argue that the likelihood of that is increasing.

We've got increasing convergence in the corporate sector, where, for example, we now have a number of media companies that include newspapers, radio, and television. They're all the same company. So the likelihood that our information gets out there, crosses the border – and we have no control over it at that point. It is used for a purpose that we didn't want it used for. What would be bad about that? Well, if it's used to come back and deny us service in a different area, for example – and insurance is the most common way you get that – or to market to us a product that's inappropriate. We don't want to be bombarded by marketing.

11:55

I don't have an answer to this question. I view it as a very serious one, and I think it's incumbent upon us to try and come up with something as legislators that starts to take some steps towards protecting our citizens because, again, if we don't, who will? The answer is nobody. I'm sure our corporations and people that are sending our personal information across the border don't mean to cause us any harm, but frankly they're kind of out of the picture here because they have no control over what happens to that information once it's crossed that border unless they exercise due diligence and say: well, we won't contract with you to provide payroll services unless you guarantee us. But as Gord has just pointed out, that option is rare, to be able to have that kind of control. So what can we do to help our citizens and help our corporations that would be sending information?

By the way, I hope that the government is cognizant when they look to reduce costs in services. I hope my colleagues on this committee are being very careful with government contracts that are sending personal information overseas to be processed because I would argue that the government has an equal inability to protect our personal information when they contract to have our X-rays read in India or, you know, our payroll done somewhere in the U.S.

The Deputy Chair: Thanks, Laurie. Good comments. I do believe that we have an obligation to our citizens to do something, and maybe this case is, you know, a further comment to the feds to do something as well.

Mr. Lund: Well, I believe this is a big issue. I thought that when the PATRIOT Act was born in the U.S., we did have some comfort and something in the federal legislation, but from what I'm hearing this morning, maybe we should have had discomfort. Was I reading that wrong?

Ms Lynn-George: Well, what happens in Alberta is that the Alberta organization that is subject to PIPA is on the hook if personal information is collected, used, or disclosed improperly. Wherever that occurs, whether it's in the U.S. or India, that organization is held accountable in Alberta. The same goes for a PIPEDA organization. If they have some sort of privacy breach, they're on the hook under PIPEDA, and the federal commissioner can investigate.

The question, I think, that is in the background here is: what jurisdiction does a Canadian government have over something that occurs? Can they do anything to that third party in the other country? That's a separate issue. What we're looking at here is how those organizations communicate that information about how their information is going to be handled by someone who is actually working for them. It's not talking about what liability those service providers have if they do something improper in another country.

Mr. Lund: Mr. Chairman, if I might, I would move that we accept number 2, that

> the act be amended to require organizations to notify individuals when they will be transferring the individuals' personal information to a third-party service provider outside Canada.

Now, I also would like us to, perhaps in some other meeting, bring this issue up and be prepared to make some recommendations to the federal government about what we would like to see them do to

further protect the information because I can see some of this flowing to, say, Toronto, Ontario. Now, we're in another jurisdiction, and then it flows across the line. I think that we need to try to do a little bit of research on: is there anything that we can do or that the federal government can do? I think we lose control, but is there something the federal government can do? Albeit that we could go after whoever transferred it to Ontario, sometimes it doesn't do much good after the damage is done.

The Deputy Chair: Ty, I've noted your motion to amend to notify individuals when they will be transferring the individuals' personal information to a third-party service provider outside Canada. That's option 2. What I will do is I'll take that second recommendation as other business for our agenda for our next meeting. It gives staff some time to prepare and discuss that. Would you be happy with that?

Mr. Lund: Oh, yes. That's what I intended.

The Deputy Chair: Okay. Thank you.

We have option 2 in front of us. All those in favour? Unanimous. Thank you.

Laurie.

Ms Blakeman: Sorry. There's just something I picked up from your last comment. Really, how likely is it that an individual would possibly be able to pursue an Alberta company to show that they lost control of that information? They would have to be proving how the international company has used and abused the information. I mean, it's an impossibility for an individual to actually bring that home and prove it to the Alberta company, so it becomes a moot protection because it's not possible to use it. It's not realistic to follow it.

Ms Lynn-George: It may be realistic, particularly given the powers of the commissioner to investigate.

Jill, would you be able to comment?

Ms Clayton: I would like to comment. This hasn't come up as a main issue in any of the complaints before our office. It has come up once or twice as a peripheral issue, and in most of those cases we found that the information did not actually cross the border, so it turned out that there wasn't an issue. There has been at least one case in our office where personal information was employee personal information, but the organization contracted to an organization, a service provider in another country, information on a laptop that was stolen. The organization did all the right things, notified the affected employees. We did end up with a complaint, that we investigated, and we're talking to the organization about what it can do in the future to notify individuals if their information might be going into the hands of a contract service provider in another country: due diligence, security in contracting, what the principal organization can do to make sure that its contractors are implementing reasonable safeguards to protect information. So there is something that we can do with the organization in Canada, in Alberta.

Ms Blakeman: But it would have to come back to the individual to be able to at least identify the path and then take it to the Privacy Commissioner to investigate.

Ms Clayton: That's right, and without notification that would be very difficult. In the case that I'm talking about, the organization itself did notify individuals affected by the breach, so that's how they knew.

The Deputy Chair: Okay. We'll cut off conversation at this time, and we'll recess for lunch and reconvene at 12:40. Is there any reason that 12:40 doesn't work for someone here? Okay. Then 12:40 it is. Thank you.

[The committee adjourned from 12:03 p.m. to 12:47 p.m.]

The Deputy Chair: Back to order. We're going to deal with item 9 on our agenda, question 11. Again, we're going to go through the summary.

Ms Lynas: The Personal Information Protection Act requires organizations to ensure that reasonable security arrangements are maintained for personal information in their possession. Even though an organization may have procedures and systems in place, privacy breaches can occur. Personal information may be lost, stolen, or compromised for a variety of reasons. It may be a computer hacker, a rogue employee who decides to release or sell data, or human error: a computer tape gets lost or a laptop gets lost somewhere. Organizations are not compelled by law to notify individuals that their personal information has been lost. There's no express provision directing organizations to notify affected individuals after a privacy breach.

In 2005 the office of the Information and Privacy Commissioner conducted five investigations related to breaches of personal information. In each case the commissioner required these organizations to notify individuals who might have been affected by the breach.

Other jurisdictions, including many U.S. states, have brought in legislation requiring notification. There's a range of practices, including notifying a government office, advertising in the media, and contacting individuals directly. Some legislation allows organizations to take into account the likelihood of harm from the specific information that's been lost.

We asked the question of whether organizations should be required to notify individuals if the security of personal information has been breached. Two professional regulatory organizations stated that affected individuals should be notified since they may have valid concerns with respect to their personal safety and so that they could make a personal assessment of risk. Another association said that individuals cannot protect themselves if they're unaware of a security breach.

Thirteen organizations supported the commissioner's risk-based approach to notification, where the need to notify and the method of notification are proportional to the risk of harm that may be experienced by the individuals whose personal information has been compromised.

Another five organizations supported notification only when there was a high risk of harm such as theft or fraud to the individual as a result of inappropriate disclosures. One of the associations stated that an organization should have discretion whether to notify when the breach does not compromise the individual's identity or involve sensitive personal information.

Another association and a business commented that individual notification of every incident would be onerous and costly. These businesses added that notifying consumers of even minor breaches might cause unnecessary panic or that consumers would ignore notices if they received too many. Individuals may not be able to differentiate between situations where there's a high or low risk.

Another association commented that while notifying an individual of a loss of personal information is a sound business practice, notifying the commissioner of a privacy breach should be a suggested practice and not a requirement.

An organization suggested that it would be more beneficial to develop guidelines or best practices for individuals and businesses rather than legislation.

Another association indicated that the commissioner should be notified in each case of a serious breach of security that is likely to result in high risk of harm to individuals.

Two other organizations stated that the commissioner should have authority to direct the organization to notify affected individuals.

One business stated that a reasonable time frame for notification is important. It should be completed in the most expeditious time possible and without unreasonable delays, permitting organizations the time needed to determine the scope of the breach as well as who to notify and how, so they can take into account the circumstances.

Another business and association stated that organizations should be able to use a wide range of notification methods.

One business cited a 2005 report by the Progress & Freedom Foundation, concluding that notification costs to all parties far outweighed the benefits. They cautioned against adopting a notification requirement without further study.

That's all.

The Deputy Chair: Amanda, are you going to do the policy paper? Jill? I've just got different notes here.

Ms Lynas: Jill is going to talk about the experience in the commissioner's office about privacy breaches before we get to the paper.

Ms Clayton: Thank you. I just wanted to provide a little bit of information for the committee's consideration. I note that in the minutes of April 20 Ms Blakeman had asked that our office provide some information about self-reported breaches but also complaints received that were not self-reported, so I have a little bit of information about both.

Again, in the total number of cases that we had opened since the act came into force, around 730 cases, the total number of those cases that were mainly focused on an information security breach as the primary issue was 75, which represents 11 per cent of all our cases. That does include 20 cases of self-reported breaches and 55 additional complaint case files.

Of the self-reported breaches four had to do with laptop thefts, three had to do with hacked databases, three had to do with break-ins and computer thefts, and there were a few others that had to do with things like paper records going missing, a lost memory stick, unauthorized access, and use by former employees. These kinds of breaches ranged from a single incident affecting one individual to incidents where literally thousands of individuals were affected by the breach.

In almost all of the self-reported breaches the organization, by the time they contacted our office, had already notified the affected individuals. In some of those cases they were contacting our office to say, "This breach has occurred," and they wanted some assistance in determining how to notify, whether to notify, what should be included in the notification, what other kinds of actions they needed to implement to prevent future breaches.

Again, in almost all of those cases the organizations had already notified or were about to notify. In one case that I know of, no notification was required. That was an organization that was operating in multiple jurisdictions across Canada and had also consulted with other regulatory offices. The information was encrypted, and the organization had gone to great lengths to demonstrate that the information could not be broken into, that it was securely encrypted, so the information would not have been available to unauthorized persons. But, otherwise, notification in all of those cases.

12:55

Of the 55 complaint case files that we opened, 34 of them had been opened after we received a complaint from an individual, so an individual already knew about a breach or was alleging a security breach. Sixteen of those case files were opened after we received referrals from Edmonton Police Service investigating other matters. There were a number of prominent investigation reports on our website where EPS had been investigating other incidents and had taken into possession some commercial paper that they had found there – credit card receipts, account collection files, things like that – in which case they had notified our office, and we had opened investigations. Another five case files were opened based on stories reported in the media or, in at least one case, where one of our portfolio officers came upon some records that had been abandoned.

Of those information security case files, where 34 complainants had contacted us, really we were only looking at one individual affected by the situation, by the incident, so there was no need to notify. The individual already knew about it, and they learned about the findings of the investigation through a letter or an investigation report. Probably the 16 case files that we opened in response to referrals from Edmonton Police Service: again, in almost all of those cases we recommended notification. I say almost because in a couple of those cases there was not enough evidence to carry on with an investigation, or we determined that it was not personal information, so we did not have jurisdiction.

Our office, certainly where the information is sensitive or could put an individual at risk for identity theft or some other kind of financial fraud, where the information is not encrypted and could be used by unauthorized persons, would strongly recommend that organizations notify individuals affected by the breach.

The Deputy Chair: Any questions?

Mr. Ducharme: Could you give me an example of when you made reference to five case files opened based on media stories? Would it be someone from your department who would notice it, or is it the public that sees it on TV and then calls in?

Ms Clayton: It could be either of those. One that comes to mind was a situation involving wireless network breach. The story was reported in the *Edmonton Journal*. It came to the commissioner's attention. On his own motion he opened an investigation.

Mr. Ducharme: Okay. Thank you.

The Deputy Chair: Thanks, Jill.

Amanda, are you ready? Go ahead.

Ms Swanek: Breach notification is a somewhat complex issue, but I am going to try to make this as brief as possible. I want to start off, though, with a few stories, and the first story might sound a little familiar. In January of this year the TJX group of companies, which owns the Winners and HomeSense stores in Canada, reported that it had suffered a major privacy breach. This announcement was widely reported in the media. Now, besides Winners and HomeSense in Canada, the TJX group of companies owns several retail stores world-wide. This privacy breach affected 45.7 million customers world-wide. In Canada alone over 250 of those Winners and HomeSense stores were affected. The compromised information included mostly debit card and credit card numbers, but in some

cases it also included customers' names, addresses, and driver's licence information.

Now, in terms of notification, Winners and HomeSense have provided a customer alert on their website, and they are also directly notifying individuals whose driver's licence information was compromised. This breach is currently being investigated by both the federal and Alberta commissioners.

Going back a little farther, in October of 2005 a Toronto newspaper reporter informed the Ontario Information and Privacy Commissioner that patient health records were blowing around the streets of downtown Toronto on a film shoot location. The cause of this breach was apparently human error. Now, a clinic in Toronto had contracted with a shredding company to have the files shredded. Apparently there was a miscommunication when the shredding company employee picked up the files, and the employee mistakenly marked the files for recycling instead of shredding. These files were then sold intact to a special-effects company working on the film.

Jill has told us a little bit about some of the cases that have come before the Alberta commissioner. Three investigations involved basically one situation where the Edmonton police had notified the commissioner that during an investigation into another matter the police had found documents from several Edmonton stores. These documents contained customers' personal information. Some of the documents were found in a motel room. Other records were turned over to the police by two individuals who had been charged with credit card fraud. The accused had found the documents in dumpsters behind the stores. This is where the store's employees had been throwing the documents out. The documents were mostly return receipts. They included credit and debit card information, customers' names, signatures, addresses, phone numbers, and some details about the purchases. Personal information from some of these receipts was consolidated by criminal suspects in a notebook that was also found by the police. There was one documented case of credit card fraud that resulted from this.

Now, in the Ontario case I talked about and in many of the Alberta cases, both the Ontario and Alberta commissioners have supported notification of affected individuals. However, only the Ontario commissioner could require that notification. This is because Ontario has an act that governs personal health information – this is similar to Alberta's Health Information Act – but the Ontario act expressly requires notification of individuals whose health information is stolen, lost, or accessed by unauthorized people. Alberta's PIPA, as you've heard, does not contain such a requirement, nor does the other private-sector privacy legislation in Canada, specifically B.C. and the federal PIPEDA. However, in a recent report from the federal PIPEDA review committee they've recommended that PIPEDA be amended to require notification of privacy breaches in some circumstances.

Getting back to our act, what PIPA does require is that organizations make reasonable security arrangements to protect personal information against risks of unauthorized access, use, disclosure, and so on. For example, company laptops that contain personal information should probably be encrypted, especially considering how often these laptops are lost or stolen. In fact, a couple of days ago it was reported in the U.K. that an accountant had lost a laptop, and the laptop contained personal banking information of a particularly high-profile individual. That would be Prince Charles. So the lesson to be learned there is that it can happen to anybody.

Even when organizations do make proper arrangements to ensure that personal information is secure and protected, privacy breaches can occur. The Ontario health records case was caused by a miscommunication at the employee level. In terms of computer networks it's often said that if a hacker really wants in, they'll find a way past network security. So privacy breaches can happen even when an organization makes a real effort to prevent them. They're a reality, and the question is: should PIPA include a requirement for notification in at least some situations, specifically where the breach could lead to a risk of harm for affected individuals?

There are a few questions that I'm going to try to answer before I get into the real meat of the issue. The first question is: what do I mean by harm? Privacy breaches are commonly associated with fears of identify theft, which is a catch-all phrase including assuming a person's identity and credit card fraud, which has been around for a long time. A name, address, and date of birth are often all that is required to gain control of somebody's identity, but identity theft is not the only issue.

A lot of personal information could cause humiliation or harm to reputation if revealed. Information about personal financial problems, for example, and information that's held by counsellors and therapists fall within the scope of PIPA. You can imagine the kind of sensitive information there that would be affected by a privacy breach. This isn't just about preventing identity theft or preventing bad credit ratings. This is about preventing humiliation and a loss of dignity. That's the possible harm, and the point of notifying individuals is so that they can take action to protect themselves from some of these harms.

1:05

I also want to clarify here what is meant by notification. It can include sending a letter to affected individuals, and it can include notice in a newspaper or on a website. It would generally include information like the date of the breach or approximate date of the breach, what kind of information was accessed, what the organization has done to minimize the damage, and it may also include instructions to individuals to help them figure out what kind of steps they can take to minimize the damage.

The last question is: what should trigger notification? Or to put it another way, just how many notices are we going to start getting in the mail? Organizations could be required to report every breach regardless of whether that breach would actually pose a risk of harm to individuals, but there are a couple of problems with this approach. One is that the public may become immune to notices about privacy breaches. Continual notification might become more of an irritant than a benefit. This is sometimes referred to as notification fatigue. There also might be a high cost to organizations who are providing this notice. Now, where a security breach poses a risk of harm to individuals, that high cost might be easily justified, but it might not be so easily justified if there is little or no real risk of harm.

There's a big difference between an organization accidently disclosing your banking information on one hand and your postal code on the other. That's where this risk of harm concept comes in. An alternative approach to this notifying in every case would be to require notification only when certain conditions are met. One of these approaches is to use a risk-based test, where the factors of each case are considered to determine whether a breach poses a risk of harm to individuals. The Alberta, B.C., and Ontario commissioners have all endorsed this approach in various publications about privacy breaches. Also, 16 of the respondents have recommended a risk-based approach. Thirteen specifically talked about the risk-based approach that has been used by Alberta's commissioner. So in creating a breach notification framework, consideration needs to be given to the issue of what triggers notification.

There are other procedural issues such as: what should a notice look like? Should there be a time limit between when a breach is discovered and when notification occurs? These kinds of procedural questions can be determined in consultation with the commissioner's

office. The paper gives some further discussion about these issues, and if the committee wants, we can go into further detail.

But there are two specific issues that are put forward for the committee's consideration. The first issue – and this won't be a surprise – is whether PIPA should be amended to include a notification requirement in the event of a privacy breach. If the committee determines that some form of breach notification requirement should be included, then the second issue for consideration is how a breach notification requirement should be enforced.

On to the first issue. Now, this is where our handouts come in. The first handout is a diagram. It looks like this. You'll see that for this first issue there are four options. One of these options is to maintain the status quo; that is, not amend PIPA to include a breach notification requirement. If you don't think a breach notification requirement should be included in PIPA, then you really don't have to go any further than option 1. The other three options are all alternatives for a breach notification requirement. If an organization suffers a security breach that would pose a risk to individuals, the organization would be required to provide notification.

The difference between options 2, 3, and 4 is who will be notified. The options are basically notifying the individuals directly, notifying the OIPC, and notifying both the OIPC and individuals at the same time. Under option 2 the organization will notify the individuals directly, and the OIPC doesn't have to be involved at all. Under option 3 the organization will notify the OIPC first and will also notify individuals if the commissioner determines, based on the specific factors of the case, that notification of individuals is necessary. The commissioner would be able to compel the organization to notify those individuals. This is the approach that the commissioner has recommended in his submission. Last, under option 4 the organization will notify both the OIPC and notify individuals at the same time. The difference from the last option I mentioned is that the commissioner is not determining whether individuals also need to be notified because individuals are notified automatically by the organization. Notifying the OIPC is more of an oversight measure in this option.

Now, going to the diagram, it starts at the point of a privacy breach. Starting at the top, we have an organization that suffered a privacy breach, and the first question is whether the OIPC must be notified. If the answer is no, then we're moving on to the left side of the diagram, towards options 1 and 2. Neither of these options require the participation of the OIPC and won't have that automatic oversight of the office. The next question on this side is whether individuals must be notified. Option 1 is the one where no notification is required at all, and option 2 is where individuals must be notified directly.

Now let's go back to the top and ask that first question again: does the organization have to notify the OIPC? This time we'll take the yes route, on the right-hand side. This leads to options 3 and 4, which both require the involvement of the OIPC and will both have the automatic oversight of the office. Under option 4 – that's the one on the far right, the pink one – the organization will be notifying the individuals automatically as well as the OPIC. Under option 3 – that's the blue one – the commissioner will be determining on a case-by-case basis whether the notification of individuals is necessary.

We've got the next chart, which is the one with the blue and coral boxes. This one goes through some of the main advantages and disadvantages of the various options. The first policy consideration, on the left side of the chart, is the commissioner's ability to compel an organization to notify individuals of a privacy breach, and as you can see, it's only under option 1 that notification remains completely voluntary. The next consideration is the delay between the time the breach is discovered and the time that individuals are notified. When individuals are notified automatically – that's options 2 and 4 – you only have that one step. Under option 3 you have that extra step where the commissioner is determining whether individuals need to be notified or not. That might cause an additional delay.

Now, the next three considerations are all related. I mentioned earlier that concept of notification fatigue, which is basically where these notices become so numerous that they're more of an irritant than a benefit. The regulatory burden basically refers to the amount of resources that an organization will have to use to comply with a notification requirement. You know, as we've heard from Jill, the OIPC has developed an expertise in the area of privacy breaches and notification, and this next consideration is the opportunity for an organization to capitalize on that expertise.

Going back to notification fatigue, there's a chance that organizations, in attempting to minimize their liability, will notify individuals of privacy breaches even when there's really no risk of harm to those individuals, but if the OIPC is consulted first – and that's option 3 – the office can help that organization determine if the privacy breach poses a real risk or not. That would likely minimize the amount of notifications an individual might receive, and this in turn can lessen the regulatory burden on organizations simply because they might be providing notification in fewer cases. Of course, if the OIPC is notified first, before individuals, the organization will be able to capitalize on that expertise of the OIPC both in determining whether a privacy breach poses a real risk of harm and in terms of carrying out the notice, what information should be included in the notice, and so on.

The last policy consideration here is harmonization with PIPEDA. As I mentioned earlier, the recent report from the federal PIPEDA review committee recommended that PIPEDA be amended to include a breach notification requirement. The approach they recommended is similar to the approach outlined in option 3. That's the first issue.

1:15

The Deputy Chair: Thank you.

Ty, you have a question?

Mr. Lund: Thank you. I've just got a question to start off with. Would it be possible as a guideline to say, "Under these circumstances you will be required to notify the individual"? The reason I bring that up is that I think that in some cases, like if it's credit card numbers, the individual needs to know very, very soon so that they can cancel the cards and do all of this sort of thing.

I guess, speaking to option 3, I should have said that that's the one I favour, but I just wonder if we can help with it. Under certain circumstances where the company that has had the breach knows full well that the commissioner's going to rule that you must notify, rather than having to have this delay, they would automatically start that process, notify both. If they go to the commissioner first, they know that there's going to be a ruling that they have to. I think there are certain conditions that could be put in there that they would do the individual simultaneously with the commissioner.

Ms Blakeman: Isn't that option 4?

Mr. Lund: No, option 4 is . . .

Ms Blakeman: Sorry. Not this option 4; the option 4 in the paper.

Mr. Lund: Option 4 suggests that they will do it in every case, but what I'm saying is that there are certain cases where a company would know that the commissioner's going to say: yes, you will be

notifying. If we were able to do that, we would also have to have the ability to penalize a company if they did not do it. If we write the legislation so that it would be number 3 but under certain circumstances where you know that the commissioner's going to rule that, in fact, they will have to notify the individuals – there will be a grey area. But things like losing credit card information, for example: I know that if mine is lost, I want to know right now, not wait for the commissioner to tell them to do it.

Mr. Ducharme: Yeah. They might max out your $25 limit.

Mr. Lund: Yeah. Well, I'm sure you would lend me whatever it takes.

The Deputy Chair: Jann, go ahead, or Amanda or whoever has the answer.

Ms Lynn-George: Just one thought: something that's turning up in a number of different pieces of access and privacy legislation is an expedited process. Rather than having two different processes, one could put in something that would expedite the process in the commissioner's office for certain classes of information so that you would continue to have one process, you know, one reporting requirement, but the commissioner deals with it more quickly under certain circumstances.

Ms Clayton: The commissioner's office would certainly support that, the idea of an expedited process recognizing the need to be very timely in terms of allowing individuals the opportunity to protect themselves. I did also want to comment that we do have on our website right now some guidelines for responding to breaches so that it's out there for organizations, key steps in responding to privacy breaches. It's very similar to a publication that B.C. has on their website and the Ontario commissioner as well, so that organizations will know what kinds of things to think about if there is a breach. Consider sensitivity. Was the information encrypted? What is the harm? All of those things so that they should have a pretty good idea of whether or not they would be required to notify.

Mr. Lund: Well, Mr. Chairman, it sounds like this is all covered. I would move that

> we accept option 3, where it would be notification to the OIPC and then the commissioner would direct an organization to notify individuals, with the proviso that there would be a fast track in certain cases.

The Deputy Chair: That's not an issue for staff? Okay.

Any comments? All those in favour? Unanimous. Thank you.

So issue 2. I have – and maybe you can help me here, Karen – in Cindy's notes "Should PIPA be amended to create an offence provision for the failure to notify?"

Ms Lynas: That's a continuation of Amanda's presentation.

The Deputy Chair: Right. So you want to get going from there, Amanda?

Ms Swanek: I'll take it from there.

The Deputy Chair: Okay.

Ms Swanek: Issue 2 starts on page 20 of the paper. It considers whether PIPA should be amended to create an offence provision for the failure to notify. There are only two options under this one. These options are presented in this last diagram here.

The first option is to rely on PIPA's current offence and penalty provisions to enforce a breach notification requirement. Currently the commissioner can order an organization to perform a duty imposed by the act. If PIPA is amended to require notification of a privacy breach, then this notification becomes a duty under the act, and the commissioner can order an organization to comply.

So looking at this last diagram, we start at the top with an organization suffering a privacy breach. The organization fails to notify as required. If we look at option 1 – that's on the left-hand side – the commissioner conducts a review of the organization. The commissioner can order the organization to provide notification, and if the organization complies, then PIPA's offence provisions don't apply. If the organization decides to ignore the commissioner's order, then the organization can be charged with an offence under the act. The penalty for an offence by an organization is a maximum fine of $100,000. The advantage to this approach is that it's consistent with current enforcement and penalty provisions. The disadvantage is that these current provisions may not be significant enough to ensure compliance.

The second option. Again we've got the organization that has suffered a breach and has failed to notify. We'll go to option 2 on the right-hand side of the diagram. The commissioner conducts a review of the organization. The commissioner then issues an order finding that the organization did not provide the notification required, and at this point you'll notice that the organization doesn't get that second chance to comply with the commissioner's order before an offence provision would apply. It would be an offence simply to fail to notify. A separate penalty could apply to a failure to notify about a privacy breach. Now, the advantage to option 2 is that it creates an additional incentive to provide notification of a privacy breach. The disadvantage is that it may be perceived as heavy handed.

The Deputy Chair: Maybe. I think everybody's phones would light up. It will be controversial, you know, if we move to option 2, but your body language tells me that you want option 2.

Ms Swanek: Fortunately, I'm not the one that has to make the decision.

The Deputy Chair: Well, I know, but what are you recommending that strengthens the act? That's my question to you. You folks are dealing with this.

Ms Lynn-George: Could I just suggest that with both options 1 and 2 there is no obligation to prosecute for an offence. Prosecutions are for egregious actions. In the case of a very egregious action of failure to notify, perhaps where an organization did the numbers and decided that they just weren't going to bother because it would be too expensive, option 2 gives you the ability to go straight to an offence provision and a possible prosecution. That's the difference.

The Deputy Chair: Jill, you have a comment?

Ms Clayton: I do. I think right now our office – and I think our submission says this – relies on good faith and willingness on the part of organizations to comply and to notify. I think that most organizations are quite willing to do that, but it is entirely possible that we will come up against organizations that don't want to do that because of the negative publicity that might come out of something like this. So I think that allowing the offence provisions to carry

over in those very rare cases where it might become necessary would be something the commissioner would support.

1:25

The Deputy Chair: Option 2?

Ms Clayton: It's your decision.

The Deputy Chair: Laurie.

Ms Blakeman: Yeah. I'm just thinking that the precedent in case law on this is going to change because before we would have forgiven an organization for not understanding that if they threw the credit card receipts in the dumpster, it might lead to problems. Now, quite clearly, we understand that it will lead to problems, and they shouldn't be doing it. So as groups become more accustomed to what they should or should not do, the bar moves up on where the line is drawn on bad behaviour. I think we need to give the most support we can to the Privacy Commissioner to prosecute on this.

Mr. Ducharme: I'm just looking at option 1, and I see it as giving the commissioner strength in terms of if someone does not wish to comply after he's made an order. To me, it doesn't seem as heavy handed as option 2. Option 2 is: you broke the law; you get fined. Whereas I see the issue that when the commissioner issues an order, if they don't comply, he still has the option of telling them to comply, to notify, and if they choose to disobey his order, then he can fine. We're talking about personal privacy information. As we've already stated in lots of circumstances, there haven't been a lot of breaches that have occurred. I'd prefer just to take it one small step rather than going, let's say, with the big mallet. But, you know, maybe we need a little bit more discussion to convince me differently.

The Deputy Chair: Well, Jann is going to do that because in option 2 the organization may be prosecuted for an offence.

Ms Lynn-George: In both cases the commissioner doesn't fine anybody. The commissioner may report it to the Minister of Justice, and the Minister of Justice decides whether to proceed with the prosecution.

The Deputy Chair: Then we nail them and jail them.

Ms Lynn-George: Well, it's not automatic in any sense in the way that, perhaps, an administrative fine that is imposed by a tribunal hearing a case would be.

The Deputy Chair: Further on your point?

Mr. Ducharme: Yes, please. I see that the third point in option 2, the yellow box, basically says that the "Commissioner issues order stating that no notification occurred." Option 1: "Commissioner issues order requiring organization to notify." I see option 1 as though the commissioner is giving a little bit of an option to that organization whereas the other one says: no; you've broken the law. It doesn't really direct them to have to notify anyone; it's just that you're guilty, not giving you that opportunity to redeem yourself to the consumer. Am I reading it right? Yeah.

Mr. Martin: Well, frankly, I'm a bit worried that that's true of crimes generally. It would be nice if a poor person went out and committed a crime and you said, "Well, maybe you'll be due, but that's up to the justice system to decide." I don't see that they should be treated any differently if it's a serious breach, and if it's not that serious, if the commissioner goes to Justice, they may say that it's not worth doing. I'm not sure why we would treat somebody that's breaking the law deliberately any differently than we would in other areas.

Mr. Ducharme: So you're a hanging judge, then?

Mr. Martin: Just a fair one.

Mr. Lund: Well, I'd lean toward option 2. I'm worried about – and I think somebody mentioned it – the possibility that rather than notify even though the commissioner said you shall, they don't do if for financial reasons. What really bugs me: whenever we have a penalty in law but someone can make money by not obeying the law, then I say that our penalty is too low, or it's the wrong law. In this case this is personal information. This could be very, very detrimental to individuals, so I would move that we accept option 2.

Mr. Martin: Right on, brother.

The Deputy Chair: Ty and Ray agree. I don't know, Laurie. Should we cancel them out or not?

I'm hearing a motion to amend the act, moved by Ty, that

> we make it an offence not to notify the OIPC or affected individuals, as decided with respect to issue 1, of a security breach affecting personal information where it's reasonable to do so.

Does that cover it? Amanda is going yes, so that's fine with me then. I'll call the question. All those in favour? Unanimous. Amanda, good work.

Okay. We're going to move on to agenda item 10, Other Business. I think we had a recommendation from Ty earlier that we do some further investigation on a recommendation to the feds on the transborder flows. Do you want to comment on that, Tom?

Mr. Thackeray: Thank you. I believe that we agreed that we would have some information available to the members for the next meeting.

The Deputy Chair: Yes.

Mr. Thackeray: We are prepared to do that whenever the next meeting may occur.

The Deputy Chair: Okay. Just a note that we'd like that included. Is there anything else that we'd like for some further information?

Mrs. Sawchuk: Mr. Chairman, if I may. The minutes.

The Deputy Chair: Oh, I know what you're going to say. I forgot to include in the motion – I said April 10, and I should have included April 10 and 20, two sets of minutes. So we need to cover the motion back to item 3(b) to approve the April 20 minutes as presented. All those in favour? Carried. That was my mistake.

Now, the most controversial issue of the whole meeting is the date. Staff and the co-chair are recommending August 8, and I want to just do a straw poll starting with you, Laurie.

Ms Blakeman: Just because I'm on the end. That's a Friday?

Mr. Thackeray: No. It's a Wednesday after the long weekend.

Ms Blakeman: Okay. Yeah, I'm good.

The Deputy Chair: Laurie. Hugh?

Mr. MacDonald: I think I'm good for that day.

The Deputy Chair: Gord?

Mr. Graydon: No.

The Deputy Chair: Ty?

Mr. Lund: I don't think that works for me.

Mr. Graydon: No. You're with me.

Mr. Lund: Yes. That's right. I forgot who my company was.

The Deputy Chair: Denis?

Mr. Ducharme: I don't have my calendar with me.

The Deputy Chair: Len?

Mr. Webber: Unsure.

The Deputy Chair: Ray?

Mr. Martin: If I have to.

The Deputy Chair: That doesn't give us the numbers we need.

Mr. Ducharme: I can get back to you shortly if I make the difference. I just have to go up to my office.

Mr. Martin: Is there another one – maybe we can do it quickly – that's better?

The Deputy Chair: We have to poll our members that are missing here, and I'll do that. At least I know that we have Laurie and Hugh.

Mr. Ducharme: I'll let you know immediately.

Ms Blakeman: Mr. Chairman, generally are we looking at Wednesdays?

The Deputy Chair: No. We're just generally looking for a day.

Ms Blakeman: Okay.

The Deputy Chair: It's to try to get just quorum and to try to get this moving, Laurie. That's my issue. With Cindy taking on new duties, you know, it kind of has to work in my calendar too.

1:35

Ms Blakeman: Congratulations, by the way.

The Deputy Chair: Yeah. Thanks.

So I can make the 8th work, but we have to have a quorum. After the meeting, anyway, if you two can check your schedules, and then we'll poll the missing members.

Anything else to cover?

Ms Blakeman: We never did the extra submission. Was that ever going to be discussed? We agreed to accept it, but we never discussed it. Or did we while I was out of the room?

Mrs. Sawchuk: Mr. Chairman, I believe what we did was we forwarded it and just asked that it be included in the analysis of the different issues by Service Alberta staff.

Ms Blakeman: Okay.

Mrs. Sawchuk: Yeah. It's in the minutes too. I did mention it in the minutes.

Ms Lynn-George: The issue was primarily PROs.

Ms Blakeman: That's right.

Ms Lynn-George: It was mentioned, and it was certainly taken into consideration.

The Deputy Chair: Jill, Tom, Hilary, Jann, Kim, Amanda, thank you. I guess we'll send a thank you to Cindy from the committee. We will let you know on the next meeting.

A motion to adjourn.

Mr. Graydon: So moved.

The Deputy Chair: Gord Graydon. All those in favour? Carried. Thank you.

[The committee adjourned at 1:37 p.m.]