Legislative Assembly of Alberta

The 29th Legislature
Second Session

Standing Committee on Alberta's Economic Future

Personal Information Protection Act Review

Wednesday, September 7, 2016
10 a.m.

Transcript No. 29-2-9

Legislative Assembly of Alberta
The 29th Legislature
Second Session

Standing Committee on Alberta's Economic Future

Sucha, Graham, Calgary-Shaw (ND), Chair
Schneider, David A., Little Bow (W), Deputy Chair

Anderson, Shaye, Leduc-Beaumont (ND)
Carson, Jonathon, Edmonton-Meadowlark (ND)
Connolly, Michael R.D., Calgary-Hawkwood (ND)
Coolahan, Craig, Calgary-Klein (ND)
Dach, Lorne, Edmonton-McClung (ND)
Fitzpatrick, Maria M., Lethbridge-East (ND)
Gotfried, Richard, Calgary-Fish Creek (PC)
Hunter, Grant R., Cardston-Taber-Warner (W)
Jansen, Sandra, Calgary-North West (PC)
Panda, Prasad, Calgary-Foothills (W)
Piquette, Colin, Athabasca-Sturgeon-Redwater (ND)
Schreiner, Kim, Red Deer-North (ND)
Taylor, Wes, Battle River-Wainwright (W)

Office of the Information and Privacy Commissioner

Jill Clayton	Information and Privacy Commissioner

Support Staff

Robert H. Reynolds, QC	Clerk
Shannon Dean	Law Clerk and Director of House Services
Trafton Koenig	Parliamentary Counsel
Stephanie LeBlanc	Parliamentary Counsel
Andrea Szabo	Legal Counsel
Philip Massolin	Manager of Research and Committee Services
Sarah Amato	Research Officer
Nancy Robert	Research Officer
Corinne Dacyshyn	Committee Clerk
Jody Rempel	Committee Clerk
Aaron Roth	Committee Clerk
Karen Sawchuk	Committee Clerk
Rhonda Sorensen	Manager of Corporate Communications and Broadcast Services
Jeanette Dotimas	Communications Consultant
Tracey Sales	Communications Consultant
Janet Schwegel	Managing Editor of *Alberta Hansard*

Transcript produced by *Alberta Hansard*

Standing Committee on Alberta's Economic Future

Participants

10 a.m. Wednesday, September 7, 2016

[Mr. Sucha in the chair]

The Chair: All right. Good morning, everyone. I would like to call this meeting to order. Welcome to all members, staff, and guests in attendance for this meeting of the Standing Committee on Alberta's Economic Future. My name is Graham Sucha. I'm the MLA for Calgary-Shaw and the committee chair.

I would ask that the members that are joining us at the committee table introduce themselves for the record, and then I will call on the members teleconferencing to introduce themselves. I will start to my right.

Mr. Schneider: Dave Schneider, deputy chair, MLA for Little Bow.

Mr. Dach: Lorne Dach, MLA, Edmonton-McClung.

Connolly: Michael Connolly, MLA for Calgary-Hawkwood.

Mr. Coolahan: Craig Coolahan, MLA for Calgary-Klein.

Mrs. Schreiner: Kim Schreiner, MLA for Red Deer-North.

Mr. Carson: Jon Carson, MLA for Edmonton-Meadowlark.

Mr. S. Anderson: Shaye Anderson, MLA for Leduc-Beaumont.

Ms Fitzpatrick: Maria Fitzpatrick, MLA, Lethbridge-East.

Mr. Gotfried: Richard Gotfried, MLA, Calgary-Fish Creek.

The Chair: For those on teleconference be sure to mute your line.

Please proceed, Mr. Hunter.

Mr. Hunter: Grant Hunter, Cardston-Taber-Warner.

The Chair: Mr. Taylor, please proceed.

Mr. Taylor: Okay. Wes Taylor, MLA, Battle River-Wainwright.

Mr. Koenig: Trafton Koenig, and I'm a lawyer with the Parliamentary Counsel office.

Dr. Amato: Good morning. Sarah Amato, research officer.

Dr. Massolin: Good morning. Philip Massolin, manager of research and committee services.

Mr. Roth: Good morning. Aaron Roth, committee clerk.

The Chair: All right. Mr. Piquette, are you on the line?

Mr. Panda: Prasad Panda, MLA, Calgary-Foothills.

Mr. Piquette: Yes, I'm here.

The Chair: Okay. Mr. Panda is present.

Mr. Hunter, you're on the line as well?

Mr. Hunter: Correct.

The Chair: Ms Jansen?

Ms Jansen: Yes, I am. Thank you.

The Chair: Excellent.

Now that we have all the Labour Day shakes out of us, a few housekeeping items to address. The microphone consoles are operated by *Hansard* staff, so there is no need for any members to touch them. Please keep cellphones, iPhones, and BlackBerrys off the table as they may interfere with the audiofeed. Audio of the committee proceedings is streamed live on the Internet and recorded by *Hansard*. Audio access and meeting transcripts are obtained via the Legislative Assembly website as well.

Up next is the approval of the agenda. Would a member like to move the approval of this agenda? Moved by Mr. Connolly. All in favour of the motion, say aye. All opposed? On the phones? The motion is carried.

We have the minutes from our last meeting. Are there any errors or omissions to note? If not, would a member like to move adoption of the minutes for the previous meeting? Moved by Mr. Dach that the minutes of the June 14, 2016, meeting of the Standing Committee on Alberta's Economic Future be adopted as circulated. All those in favour, please say aye. All opposed? On the phone? That motion is carried.

The committee is hearing oral presentations today with respect to the review of the Personal Information Protection Act. I would like to welcome our first guests here.

Before we hear from our guests, I will begin with a quick overview of the format for today's meeting. Each group will have 10 minutes to speak, and following all presentations on a panel, I will open the floor for questions from committee members.

Members, I will follow our usual practice of alternating between opposition and government members, and I would suggest that members keep their questions to one plus one supplemental each round. Members can be added back onto the speakers list if they wish. Members on the phone, please e-mail or send a Lync message to our committee clerk, Aaron Roth, if you wish to be added to the speakers list as well.

We will be beginning with our first presentation, by the Calgary Chamber of Voluntary Organizations. Please proceed.

Calgary Chamber of Voluntary Organizations

Ms van Kooy: Thank you, Mr. Chairman. Mr. Chairman, ladies and gentlemen, my name is Katherine van Kooy. I'm the president and CEO of the Calgary Chamber of Voluntary Organizations, and I'd like to thank you for this opportunity to be able to speak to our submission and specifically to the question as to whether PIPA should be extended to include the activities of all nonprofit organizations. Nonprofit organizations are considerably affected by the regulations outlined in PIPA, and I'm here to speak to and give voice to some of their concerns.

Now, the Calgary Chamber of Voluntary Organizations, or CCVO as we are more commonly known, works to promote and strengthen the nonprofit and voluntary sector by developing and sharing resources and knowledge, building connections, leading collaborative work, and giving voice to critical issues that affect the sector.

One of our key functions is to provide leadership on issues that have a broad impact on organizations in our sector, issues such as this, that are often beyond the capacity of the individual organizations to really be able to engage in. In that role CCVO was very involved during the review of the legislation in 2006-2007 to try to understand and identify the implications of the proposed extension of the Personal Information Protection Act to cover all Alberta charities and nonprofit organizations at that time. We found that actually to be a very informative process because there were a lot of concerns raised and almost an immediate reaction opposed to the extension of the legislation, and our involvement in that process was really quite informative for us.

More recently, as the review of the legislation once again came forward, we gathered input from a number of focus groups, the

Calgary-based organizations, to give us an idea that enabled us to clarify their issues and concerns, and that input combined with our research forms the basis for our recommendations.

Now, our position is that we have supported the extension of PIPA to cover all Alberta nonprofit organizations. We did that in 2007 when the change was not made, and that is still our position, notwithstanding concerns that any extension of PIPA needs to be implemented with a full understanding of the challenges it poses, particularly for small organizations.

Now, our support for the extension and the inclusion of all nonprofits under PIPA is based on several reasons. First, it's our belief – and it's certainly the position of many of the organizations that we've heard from – that on the part of the public there's a sense that their personal information needs to be handled with due regard for their privacy; that nonprofit clients, members, or patrons we don't believe distinguish between how their personal information is handled, whether it's handled in one way by government or by the private sector; and that there's a different standard for information that's handled by nonprofit organizations. That's our fundamental position.

Many organizations already comply with privacy legislation, including PIPA. That applies for those nonprofit organizations that are engaged in what's defined as commercial activity. Other organizations are subject to privacy legislation under the Health Information Act or the Freedom of Information and Protection of Privacy Act.

There are many other organizations that might be technically exempt from the legislative compliance, but they've chosen to adopt the standards voluntarily. They've done that frequently just because they see it as a good business practice. We also heard from a number of organizations that participate in our focus groups that they found that it was easier to simply comply than to try to determine whether or not they were required to comply, generally because of the difficulty in interpreting the language around whether or not they were engaged in commercial activities. I'll speak more to that later on.

One of the other concerns that we have is that with so many nonprofit organizations outside the coverage of this legislation, the employees and volunteers of those organizations have no recourse through the office of the Privacy Commissioner to address their concerns related to the collection, the storage, or the disclosure of their personal information. If they feel that there are errors, they have no way of requiring or being able to request the Privacy Commissioner to intercede on their behalf in order to make corrections to that language, and we feel that this lack of protection for a particular class of citizens is really unacceptable.

Finally, the current exemption limits the mandate of the Privacy Commissioner to address issues involving exempt organizations or to work in a constructive manner to improve their practices with those organizations that are exempt, so it simply doesn't have the mandate to engage with them if there is a problem. For those reasons our recommendation is that PIPA should be amended to apply to all nonprofit and charitable organizations and their activities in Alberta.

10:10

But having said that, we also believe it's essential that if the current exemption is removed, there must be adequate provision to deal with the diverse nature of the nonprofit sector and the very real challenges that the legislation will pose for many organizations. I think it's often not appreciated, just the incredible diversity of this sector, but it's comprised of organizations of many sizes with a huge array of different mandates and capacities. They range from large professionalized organizations like hospitals, colleges, major human service organizations with hundreds of staff or thousands, even, to small, completely volunteer-driven organizations.

The major concern about the extension of the legislation is around the impact on the thousands of small organizations who may have at most one or two staff or rely entirely on volunteers to operate. Their lack of capacity to comply with additional regulatory requirements is a serious concern that needs to be addressed. The position of the office of the Information and Privacy Commissioner is that this constituency is similar to the small and medium-sized business organizations that they currently deal with. We feel that that position reflects a critical lack of understanding of the nature of small nonprofits.

The volunteers that run the thousands of small organizations are driven by a passion to support a certain activity or a service in their community. They come with a wide range of backgrounds and experiences and abilities, and often – most often, I'd say – they have limited time to commit. Concerns about having to spend time understanding and complying with more legislation compose a real deterrent to recruiting and to retaining volunteers. There's a lot of change as staff members and volunteers join and move on from these organizations. Organizations are established and they close down, so relying on institutional knowledge is really not a reliable expectation in terms of ensuring that compliance with the legislation is actually addressed.

Therefore, we recommend that PIPA not be extended to include exempted organizations unless there is a clear commitment to implement a robust and ongoing information and training program to assist organizations to understand the requirements of the legislation as well as to provide the resources that will enable them to comply as easily as possible. We recommend that the implementation of the extended legislation should occur over an 18-month transition period, which is longer than what's been proposed, in order to educate and support organizations affected by the change. We also recommend that OIPC implement a robust education and training program and work with umbrella organizations, not exclusively but as one vehicle, to understand the educational needs of nonprofit organizations. Thirdly, education and training must include plain-language explanations around information collection, retention, and disclosure; definitions of reasonableness; and a very simple checklist for organizations to be able to track compliance requirements.

The last point that I'd like to address is the challenges posed by inconsistent use of terminology across different pieces of legislation and the difficulty for the layman to understand common legalistic language. We heard from organizations in our focus groups again about the frustration from inconsistent or unclear definition of key terms. I think that's been pointed out previously as well. For example, for nonprofits the distinction as to whether or not many of them have to comply with the existing legislation is whether they're engaged in a commercial activity, but "commercial activity" is not very clearly defined. When organizations need to spend a lot of time trying to figure out whether or not the legislation applies to them, I think that's really problematic, and they shouldn't have to engage a lawyer in order to try to get an interpretation as to whether it applies.

But it's not just the problems within the individual legislation, within PIPA, but also the inconsistent use of terminology across different pieces of legislation. I know this is a broader issue in terms of legislative drafting.

Other organizations have raised concerns . . . [A timer sounded] Sorry. You've got my notes.

The Chair: I apologize to interrupt here, too. There will be some room for questions afterwards as well.

Ms van Kooy: Thank you.

The Chair: I will now move to our next presentation, the Edmonton Chamber of Voluntary Organizations.

Edmonton Chamber of Voluntary Organizations

Mr. Dahms: Thank you, Mr. Chairman and members of the committee. I agree with my colleague from Calgary that we should look to extend the provisions of the act to include nonprofits and charities but with caution and consideration. I guess the first thing I just want to emphasize is: let's understand the scope. This includes organizations in our province that are incorporated under a variety of acts: the Societies Act, the Religious Societies' Land Act, part 9 of the Companies Act, the Agricultural Societies Act, and so on.

The count that's been offered for organizations incorporated under the Societies Act is north of 20,000 organizations, so we're talking about a lot of people, a lot of Albertans who are involved in these organizations providing service every day. Certainly, I think the expectations of Albertans since this act first came into force have evolved with the world of online shopping and all the other kinds of things and concerns about identity theft. I think we need to understand that Albertans do have expectations about how their information is protected, so I think a consistent and even approach is a good one.

But I certainly want to emphasize Katherine's point – and I think you'll hear this point with other presenters – and that is trying to make this simple and not burdensome. You have organizations that are run solely by a group of volunteers who have lives, have children, have all the things that we have as families, and to get folks tied up in lots of complications around this sort of activity really isn't beneficial. Certainly, the point made about critical training and support, making this simple, making the language plain, making it really clear: these are the things you need to do, at minimum, to ensure that what you're doing as an organization protects the information of those who are your members or your volunteers. That is really, really important.

Katherine alluded to another point. There are many nonprofits that are under contract with Alberta Human Services, particularly, providing client services on behalf of the government. They have requirements under the Health Act and other legislation to protect the information of their clients, and it's a higher order of protection. I've been speaking to colleagues about this, and their ask was that should this provision be made to draw organizations in under the Personal Information Protection Act, efforts be made with the education and training to help organizations that have a higher order of responsibility understand how this all blends together. So if I have this responsibility under this act and a different responsibility under this act, what's my deal? I think it's really trying to help blend those things together, too, for those organizations who are providing, again, client services where there is a higher order of protection that's necessary.

I think my closing comment simply is this. I've observed, as I've been going to meetings with many nonprofit organizations, that without some sort of standard or common practice that's recommended or in force in some measure, folks invent their own. I've seen all kinds of different and very interesting processes used at meetings and in other sorts of activities of organizations where there is a notion that we need to do something here to protect the information of people, and how that's done is really quite marvellous, remarkable sometimes.

I think that by providing at least a common, minimum approach, it may be beneficial to the organizations to find that ground that they need to stand on in order to really do best practice. I think this is less about coming up with a whole stack of rules than it is about: let's apply some common sense and do some things that make sense in a way that's sustainable. I think that's really key, to be able to come up with that sort of solution that enables us to go forward into the coming years and make it simple for organizations to do the right thing when it comes to protecting the information of their members and their volunteers.

Thank you.

The Chair: Excellent. Thank you very much.

We will move to our next presenter, which is the Calgary Urban Project Society. Please proceed.

10:20

Mr. Perry: Hello. You guys have been blacked out the entire time. I don't know if that's intentional.

The Chair: Could you see the previous presenters?

Mr. Perry: No. During the preliminary aspects of this we could see you all, it was all good times, and then suddenly it went black. But that's okay. It was just more for information than anything.

Calgary Urban Project Society

Mr. Perry: I'd like to introduce myself. My name is Robert Perry. I'm the senior director at Calgary Urban Project Society, or CUPS. My colleague is Emily Wong, and she works there as well.

CUPS is a charity in Calgary, and we look after the most vulnerable people in the city. We have health, education, and housing programs, and we strongly believe in looking after the most vulnerable. We realize that we cannot do it alone, that there's no one solution to solving some of the issues that people have, so it means we have to work together. The other one is that we have to think about new solutions and supply some ingenuity in how we're going to get things done.

I believe you have this PowerPoint in front of you, so I'm not going to just go through it; you can look at it at your own pleasure. In terms of privacy a lot of our participants, of course – think of a homeless man or a homeless woman, some families, that sort of thing – would have some mental health issues and their own definitions of what privacy is as well.

We also work across multiple different professions, so we have nurses, doctors, social workers, a plethora of different ones, and they all have their different rules and regulations that they need to follow, and then, of course, there's all the different privacy legislation that people have to act under. We also have to work across international boundaries. We have databases that are developed in the United States that we use that are stored in Canada, so we have international privacy legislation that we have to be concerned about. All this is with the backdrop of being focused on: what are the best needs of our participants?

So we are setting up a part of our organization that is removed from helping people in the sense that they have to devote some of our time, treasure, and talent to looking after these things, which we believe passionately are true and need to be done, but it takes away the resources from the people that we help. Our focus is on helping those vulnerable people, and it's always painful for us when we have to devote more time and resources to looking after legislation and things.

On the third page of our thing there's some of the legislation that we have to pay attention to. Working with my colleagues, virtually none of them understand any of these. They are not lawyers. They're nurses who do excellent foot care or women's health care or gynecological services, or they're wonderful teachers who are

looking after children with severe disabilities, or they're social workers involved in domestic violence situations. Their expertise is not in understanding legislation.

They also have their own professional ethics that they have to follow. Curiously or interestingly enough, these ethics are the ones that they hold most dear to their hearts, not the legislation, so they will revert to what their ethical body will say, so the Alberta nursing federation or something like that. Those ethics are slightly different, so they get into conflict when they're trying to share information that is in the best interests of the child or the best interests of the participant. But those things all come together in a conversation when we're trying to help somebody. So it's a hodgepodge of things that people don't really quite understand.

I loved the presenter from Edmonton, that people make things up when they don't know. When they're young and they're starting their job, they hear from their manager, "This is what the legislation says," and that could have been 20 years ago, and nobody has gone back and been able to reread it, understand it, and apply it because it may have changed or not changed. So the thing is that there are these great rules out there. I love them. In fact, the Children First Act I think is a beautiful piece of legislation because it does make it very clear that the child's health and safety is first and foremost. But there are all these things out there that people – it's hearsay. They may be clear in the sense of looking at them one by one, but in the jumble of applying things and being ingenious, they come out very messy sometimes, and these laws and rules are getting in the way of helping people.

Our position here, in the end, is just to clarify these things, to make them simple, to make it that one supersedes the other so that it can be very easily understood which ones we have to pay attention to, which ones have primacy, so that there's a hierarchy of rules that we can follow and have a very good, robust, continuous education process. So when I get into conflict with a colleague and they say, "No, this is right" or "That's right," we can go phone some smart person, and I know they do exist in the government because I found one the other day to help me answer a question.

That's basically what we have. We have multiple different rules we have to apply. We don't know which one is on top. We'd like to get that sorted out and then have continuous support for people as they apply these things.

Have you got anything to add, Emily?

Ms Wong: No. That's good.

Mr. Perry: No? We're all good. Thanks.

The Chair: All right. We will now proceed with the Federation of Calgary Communities.

Federation of Calgary Communities

Ms Evans: Thank you, Mr. Chairman. My name is Leslie Evans, executive director with the Federation of Calgary Communities. Thank you for inviting us to speak on this issue today.

The federation was created 55 years ago as a result of about 36 of our community associations wanting an advocate or a voice for their work. The community association network now, today, consists of 150 geographically based associations here in Calgary. We have the largest volunteer network, with 20,000 volunteers serving in our community associations here in Calgary alone. The federation's membership has also grown over the past decade due to our work around not-for-profit governance and financial audit. We now have about 220 small, community-based not-for-profits within our membership. About 90 per cent of these organizations have one common trait, and that's that they're exclusively run by volunteers. This fact is central to our position.

Community associations are incorporated as independent, member-based, not-for-profit societies within the province of Alberta, under the Societies Act for the most part. They share a collective mandate of offering social, recreational, and educational opportunities to meet real community needs. They're also a voice for community life.

Our network is full of passionate, community-minded volunteers who donate millions of hours each year to offer programs, services, and advocacy work for their residents. More than 1,800 volunteers hold leadership positions on community association boards. These volunteers are willing to step forward because they want to create a sense of belonging for themselves and their families and want to enrich the quality of life for their neighbours. They soon realize, however, that the responsibility of being a director is far greater than having fun with their neighbours and engaging in activities.

As governors of any type of not-for-profit, volunteers are under increased pressure to be more accountable, to understand the complexities of various compliance matters and legislation, and they serve in positions of legal responsibilities that often extend beyond their understanding and skill when they are elected to a board. Our volunteer directors not only work hard to understand good governance, but many are tasked to build new assets and amenities, fix aged infrastructure, maintain operations, engage residents on community matters, deliver front-line services and programs while keeping abreast of the ever-changing community needs and demographics. As not-for-profit board volunteers the learning curve is incredibly steep.

To help support our members, the federation provides a wide range of capacity-building services for our community volunteers, including one-on-one consultations, resource and referral network based learning, tipsheets, and free workshops that speak to governance, compliance, and operations. Our membership requests for support are steady and constant, and through daily interactions with our volunteers looking for support, we know that our role of educating is never over due to volunteer turnover and lack of paid staff. In fact, we have found that there is very little organizational memory within our membership, which creates all sorts of challenges not only for them but for us. It sometimes feels like *Groundhog Day* in terms of our ongoing training.

We believe, as do most of our members, that the protection of people's personal information is of the utmost importance. In fact, when PIPA first came out, we worked with our members to develop policies as best practices, and we have them on our website today to help them understand it, not because we had to comply – most of us don't do commercial activity – but because it is a best practice. We've also had PIPA educators out for workshops to help our members understand the importance of collecting and storing data to ensure privacy.

In theory, yes, all not-for-profits should be equally held up to PIPA legislation. However, in reality, being fully compliant with PIPA is a practical consideration not to be taken lightly. With all the nuances and complexities within PIPA and with limited human resources, high volunteer turnover, the need for affordable technology, and the lack of formal systems for data storage, we question: how will small to mid-size not-for-profits that are volunteer run implement and comply with the full legislation?

10:30

For example, when surveying residents on needs and wants, e-mailing residents a newsletter, or registering people for free events, our members use shareware or cheap online programs like SurveyMonkey, Eventbrite, PayPal, and MailChimp. The current

legislation requires that when working with third-party service providers outside of Canada, they need to find out about the provider's privacy practices and have them available upon request. Personally, I know this won't happen. In fact, they just don't have the people power to invest in that kind of research, nor do they have the resources, the funds to maybe choose differently.

Another example is around the capacity of volunteers to reply in a timely and adequate manner to a request from someone with regard to their personal information. First, due to the absence of office staff, volunteers don't always answer the phones or return e-mails in a timely manner. Therefore, they might not be able to reply to a request in the mandatory time frame. Second, often the records are not located in a convenient place. Oftentimes they are in storage because of the lack of a physical office space. The risk within PIPA is that if an organization doesn't respond in a timely manner, PIPA will treat the lack of response as a decision to refuse the request, when in reality it could just be about logistics or about capacity. This could then result in a full investigation, leaving volunteers having to muster the human resources to respond, which could cause a huge administrative burden. This could be further complicated if the volunteer who was responding to the question leaves their position prior to the resolution, again, potentially resulting in the loss of continuity and the inability of the organization to finish the complaint.

We've considered if PIPA were to refine the current list of exemptions to take into consideration volunteer-run organizations; for example, if you didn't have paid staff, you were exempt. It would be our belief that adding further exemptions would be even more confusing. For example, if we added a paid staff, we'd all of a sudden be, you know, having to comply, and what if that paid staff was only a cleaner? It can add to your administrative capacity. It added the role of cleaning a hall or something like that.

Too many exemptions or exemptions that require interpretation add to the complexity of the legislation. If full compliance for the current nonexempt not-for-profit is decided upon, then, as my colleagues have said, plain English and ongoing training will be required to support all the not-for-profits, and I would ask that we be mindful that volunteer not-for-profit organizations require simplified, streamlined processes to support their ability to comply.

Quite honestly, if the full PIPA legislation is required within the not-for-profit sector, the federation believes there will be a low compliance within our own membership. In fact, in talking to some of our members, that's what they've said. It will also give volunteers one more reason to not want to take on board positions or not to stay in those positions, which is already a huge challenge within our membership. The penalty of not complying in the current legislation is also prohibitive, which puts board volunteers in a very awkward place despite the fact that there have been no charges laid pursuant to PIPA to date.

In discussing compliance with PIPA staff, they assure us that there is a low risk of a complaint and an even lower probability of being fined. However, as a support organization that educates our members on compliance matters and other best practices, the federation is not in a position to suggest to our members that there is a low probability of being fined, so do what you can. Quite simply, adding the full legislation to their plate will leave members feeling overwhelmed and frustrated.

We understand how larger, established not-for-profits and charities with greater capacities or those working with vulnerable populations want PIPA to apply across the board. The reality, however, is that the not-for-profit sector is not equal. By removing the exemption for all not-for-profits, PIPA is presuming that all have the capacity to comply, which is far from the truth. We do not believe any stakeholder regulatory body truly wished to apply undue administrative burdens on grassroots volunteer groups. We believe that in spite of modern concerns towards privacy protection, continued education on prudent standards of practice will suffice. Therefore, it would be our recommendation to not fully add not-for-profits to PIPA but, rather, leave it as it is.

Thank you for your time and your continued consideration of volunteer not-for-profits during your deliberations.

The Chair: All right. Thank you very much.

I will now open it up for questions from the committee members. Mr. Coolahan.

Mr. Coolahan: Thank you, Chair. I have a couple of questions for the CCVO if that's okay. In your submission it was stated that one of the issues with the current legislation is that the Privacy Commissioner is unable to address concerns raised by members of the public, clients, volunteers, or employees around the collection, retention, and disclosure of information. Given that CCVO's membership is large, 350 nonprofit organizations, how often does the collection, retention, or disclosure of information become an issue, and can you provide an example of when it worked well when the Privacy Commissioner was involved?

Ms van Kooy: Actually, I'd have to defer to the Privacy Commissioner's office, if they've ever been engaged in that kind of activity. Our comment is that for exempted organizations, our understanding is that because they are exempted, the Privacy Commissioner has no mandate to intercede if there is an issue. So we're really saying that if the legislation provides a framework that allows the Privacy Commissioner to work in a constructive and collaborative way to try to redress problems with an organization that may really be causing problems in terms of how they handle the information, they have no opportunity to do that if that organization is exempt. It's to give the Privacy Commissioner a broader mandate and as well for the organizations to be able to have the opportunity to work with the Privacy Commissioner because they fall within their mandate.

Mr. Coolahan: Thank you.

Do I have time for a few more?

The Chair: Yeah. For sure. Go ahead.

Mr. Coolahan: How do you think the need to comply with multiple pieces of privacy legislation affects the service delivery of these nonprofits?

Ms van Kooy: You know, I think that's the point that's been made by a couple of the other presenters.

Mr. Coolahan: Sure.

Ms van Kooy: And I think that's a really valid point. I think the challenge is that, certainly, as Leslie said – and our organization takes the same position. We advocate that people adhere to the law, and when there are multiple pieces of legislation and when the legislation is often not integrated – it's been developed at different points in time – as Robert said, there's not necessarily any idea as to which is the prime piece of legislation that people need to respect. If they're diligent, they can spend time trying to figure out their way through what's a complex maze, and it's probably not the best use of an organization's time and energy and money. They may have access to pro bono legal advice, or they may seek advice and pay for it, but I think it detracts individuals running these organizations from their primary purpose, and I don't think that's the intent of the legislation.

Mr. Coolahan: Thank you.

You touched on this in your presentation, the 18-month transition period in order to allow for education and training. Can you elaborate a bit on what that education and training might look like?

Ms van Kooy: Well, one of the reasons that we recommended a longer period of time – as I mentioned, back in 2006-07, when the legislation was being reviewed, we were working actually quite closely with the office of the Information and Privacy Commissioner to work on developing resources that could be used to help educate organizations about what the implications of the extension of the legislation would be and tools that they could use that would facilitate compliance with the legislation. Just knowing from that experience the length of time it took to work together, I think that if the legislation is extended again, there should be consultation with organizations that can provide that kind of broader perspective about, you know, the kinds of issues that Robert has raised and that Leslie has raised and Russ as well. Realistically, a year is a pretty short period of time to work at putting that together and getting it in place and rolling it out.

10:40

Mr. Coolahan: Thank you.

Just one last quick question. One of the other recommendations you had was to ask the government of Alberta to use consistent language across the similar legislation. Maybe, for all of us, can you give us a few examples of that?

Ms van Kooy: Well, the one term that certainly has come up in this case is around the definition of commercial activities. It would be great. I can't name you right now all the different pieces of legislation where that may be defined, but it's not defined in a consistent manner. A number of organizations that have raised that with us have looked at it. In the privacy legislation it's not very clearly defined what is commercial activity and what isn't. I'm sure organizations could work with the Privacy Commissioner's office to try to determine that, but it would be really helpful if legislation was quite clear so that there wasn't always this grey zone and this matter of interpretation.

I think Leslie's point to this – and I know I've seen this with my board and I've seen it with many organizations. We all also do a lot of work in terms of training people around compliance issues. But people are very concerned about the penalties provided in the legislation, and it's very difficult to actually stand and up and say: well, forget about that because it's not actually going to apply. If you're the ED of an organization and you're faced with the potential of a substantial penalty if you're not in compliance, it doesn't make you feel very comfortable if you know that you're not in compliance, nor your board if they know that and they know what their personal obligation might be. You know, those kinds of things act as a real deterrent. Anything that you can do to make it simpler for people to comply: the easier, the better it is because it removes a lot of the other concerns that don't necessarily have to be there.

Mr. Coolahan: Thank you.

Thank you, Chair.

The Chair: Are there any questions from those who are on the phone?

Okay. I'll open it up back to the table. Member Connolly.

Connolly: Thank you very much. My question is for Ms Evans. In your submission you mentioned that although exemptions are appropriate, they create a fractious understanding of what can and cannot be applied to legislative standards. Can you explain this a little bit more in detail, please?

Ms Evans: I think it goes back to interpretation. You know, when there's an exemption around, for example, the commercial activity, is renting a hall a commercial activity? Then we get into a debate about whether that's actually in definition a commercial activity. I think it creates tension within boards. It creates kind of the need for an interpretation and then risk. I think that just causes a lot of confusion and tension. It's either all or nothing; otherwise, we're needing lawyers to interpret things for us.

Connolly: Right, as I can imagine. I know in my communities that it's incredibly expensive whenever they have to hire a lawyer for absolutely anything.

Ms Evans: Yes, absolutely.

Connolly: And just one follow-up if I may. Have you faced any challenges in service delivery or information sharing while using consent for the collection, use, and disclosure of personal information?

Ms Evans: Have we ourselves, the federation, or our membership?

Connolly: Or your membership. Yeah, either one.

Ms Evans: Well, interestingly enough, to the first question that happened. We have had an inquiry, a complaint filed through the commission from a disgruntled employee of one of our member organizations, and it was a very educational process. We did have a PIPA policy in place, and although the commission didn't have a mandate, they certainly did follow up with the complaint, chatted with me about our policy, helped me, you know, understand a little bit more, because the commercial activity we are engaged in is financial audit service. We had a very good chat, and although my policy was robust – and she said she had no jurisdiction to do anything if I wasn't in compliance – it was very helpful to have that feedback and to have that support. I guess that's the only concern I know of. None of our members have come to us saying that they've had concerns, so I have limited experience there.

Connolly: Okay. Well, thank you very much.

The Chair: Mr. Gotfried.

Mr. Gotfried: Thank you, Mr. Chair. I just have a few questions, Katherine, with regard to the CCVO presentation. You asked for a little bit more time, which I think is fair and reasonable given the breadth of the organizations involved, and I think that that would make some sense. I would maybe just like your input on what good education practices might look like for your organizations, your member organizations, and how we can make that both robust and comprehensive for you in helping people understand. What kind of processes and resources do you foresee to assist you with that?

Ms van Kooy: I think there are a number of things. To start with, I think it needs to be a program that articulates very clearly what difference the extension of this legislation will make for organizations that are currently exempt. I think an educational program will have to be made available on a very broad basis, however that's done, probably using multiple different approaches. We deliver a lot of our training in person on-site, but that's not the only way of doing it. It could be through webinars. It could be a range of different approaches. I think it would be most effective if much of that work was also done through, for want of a better term,

umbrella organizations, whether it's recreational or – there are a lot of provincial bodies that have connections to many of the organizations that currently wouldn't be required to comply with the legislation, and they would be a great way to work through those organizations to access their memberships.

I think the other point would be that the education process can't be a one-year process. As Leslie pointed out, and we've found this, we do a lot of training, for example – I know Russ does as well – around compliance for charities with the regulations through CRA, and people turn over. You know, you have change in financial people in an organization or a change in a CEO, so it needs to be an ongoing program. I think it would be a real disservice to make this extension, think that it is a relatively short-term commitment in terms of an educational program.

I think it needs to be viewed as: in the first place you need to develop the resources, and people often talk about a checklist, something that makes it simple. It's a one-pager; a small organization knows what they have to do. They can pass that on to the next person, who takes over that responsibility. Simplify it as much as you can, but don't look at this as something that gets done in 18 months and then you're finished with that obligation or responsibility in terms of the training because that wouldn't serve the purposes of this particular community.

Mr. Gotfried: It sounds like maybe some webinars in the early processes and maybe some online training and orientation type tools would help for you.

Ms van Kooy: Yeah.

Mr. Gotfried: That's great. I think that that helps to clarify maybe some of the needs that we have.

The other one that you talked about was the clarity around commercial activities and other activities, and I think maybe just for the benefit of the committee here – you know, many of us may have had some involvement with social enterprise and various things – you could give us some examples of what your organizations, the representative organizations, would consider commercial activities and maybe some that you would say require some greater clarity to give you separation of whether those are going to be categorized in that way.

Ms van Kooy: Yeah. You know, that's really an interesting question. What would people consider? As Leslie said, she deals with community associations. A lot of community associations rent out their facilities. It's a way of generating revenue. So if you rent your facility to host a flea market, is that a commercial activity? If you rent it to – I don't know – Girl Guides and they use your space, is that a commercial activity? What are those parameters? I know that we've just looked at it in terms of CRA regulations for charities in terms of commercial activities, and, boy, it's not always very easy to tell.

We offer, for example, as an organization training sessions. Are our training sessions a commercial activity? When we collect information about people who register for our annual conference, does that then punt it into the category that it's a commercial activity? I wouldn't have considered that that was the case, but it shouldn't be a matter that you have to spend a lot of time thinking about: oh, my gosh, is this or isn't it? It should be fairly clear whether it is or it isn't, and at the moment it's not.

10:50

Mr. Gotfried: So it sounds to me like maybe we need to sit down with organizations like yourselves and get a bit of a laundry list of where you already feel you've got commercial activities and some of those ones where you lack clarity. I know that we'll never be comprehensive, but it sounds like we have a lot of work to do in understanding what that list looks like for you and where the questions are: whether holding a fundraiser is a commercial activity, whether, as you said, some of the social enterprise or just regular use of facilities and revenue-generating activities are considered part of that as well. It sounds like we need some clarity to deliver this legislation to you so that you're not constantly having to pick up the phone and maybe wonder whether you're in breach of it as well.

Ms van Kooy: And that only applies if the legislation remains as it is. If the legislation is extended, it becomes a moot point because then it applies to all organizations. It's that definition of commercial activity. For many organizations that are currently exempt, it's based on that they're not engaged in commercial activities.

Mr. Gotfried: Okay. Sounds like we need some clarity there. Thank you.

Thank you, Mr. Chairman.

The Chair: Mr. Taylor.

Mr. Taylor: Yes. Thank you. First of all, I'd like to say thank you to the people that are here with the volunteer organizations for all the work they've done. There are just countless volunteers throughout this province that have put in probably millions of hours volunteering their time freely, so I wanted to start off by saying thank you to the people that are coming here today.

Anyway, to Leslie Evans, I was going to ask the question. I know you said that you fear there would be a lot of low compliance and a loss of volunteers as a result if it's too restrictive or if there's too much. I have another question, you know, that kind of goes with that statement. With regard to third-party service providers, if organizations subject to the Societies Act are made subject to PIPA, what kinds of exemptions would you propose in order to make that section practical and workable?

Ms Evans: I think adding more exemptions really just causes more confusion. I guess I wouldn't suggest adding more exemptions to try and clarify things. I think it will just muddy the waters even more.

The loss of volunteers and the low compliance. In talking with our members, most recently we had to roll out the antispam legislation, CASL, and we tried to communicate to our membership what CASL was. We drew up an implementation plan. We helped them with policies. I mean, the feedback we got was: "This is all too much. We can't do this. We don't have systems. We don't have that." When I started talking about PIPA, I basically got the same result. You know, people say to me: "We're just volunteers. We can't do this." I know that's not an excuse. My comeback to them all the time is: "But you have the liability of having to do this. You're not just a volunteer. You are a director that has responsibility." It does take away from their capacity to do what they've come to volunteer to do, to provide the programs and services, to provide a community facility for the greater good of the community. I know people will drop off as a result of this, as we saw with CASL as well.

Mr. Taylor: Because you fear that people are going to drop off as a result of this, what recommendations would you make to PIPA for more practical nonprofits and community organizations?

Ms Evans: Well, I think leaving it status quo is our position because promoting best practice – and, you know, certainly having

the commissioner continue to do education workshops upon request and that I think is the most optimal for my groups. If we go to the full implementation of PIPA across the sector, I fully support what Katherine speaks to, which is good education practices and it being an investment over the long term, much like the AGLC game workshops that frequently do their road show. I think webinars, the checklist are great ideas because then people can see if they're in compliance. We could then help implement it. I think working with capacity-building organizations like ours and CCVO and that is a good way to understand some of the education needs and the ongoing education needs.

I would certainly suggest that what Katherine is saying is what would be needed, but this would require a big investment by the province and also understanding the capacity of our organizations. We do 54 free governance and financial management workshops a year with about four staffpeople delivering those, so our capacity ourselves is stretched to add yet another one. We do a compliance workshop that takes two hours, and we don't even cover half – we cover the basic stuff that's required by our community associations.

Mr. Taylor: Do you feel that government does an adequate job of providing information on the responsibilities for your voluntary organizations to meet PIPA requirements?

Ms Evans: Currently?

Mr. Taylor: Yeah.

Ms Evans: No.

Mr. Taylor: No. So what would you like to see?

Ms Evans: Well, I think we would need to see workshops, webinars, in person, tipsheets, plain and simple language that really helps them understand what it is that they need to comply with and how they can do that easily and maybe even, you know, some resources to help them comply. I'm talking about databases. Maybe even a list of approved kinds of shareware might be helpful. I mean, it dawns on me that maybe I should be finding that out for them, knowing that they're all using those, like SurveyMonkey and that, so maybe acquiring those privacy pieces, giving them tools so that they don't have to go search and they've got a list of what software has acceptable privacy rules or complies.

Mr. Taylor: Well, thank you, Leslie. That seems to make sense.

The Chair: Member Carson.

Mr. Carson: Thank you very much, Chair, and also thank you to all the volunteer organizations that have joined us today. It's really important that we get your feedback to ensure that what we're doing here in this committee doesn't hinder your ability to serve the community. Also, once again thank you to everyone that is involved with voluntary organizations.

My questions today are for the Edmonton Chamber of Voluntary Organizations, my first one being: I'm hoping that you can elaborate on some of the organizations that you do represent and what their opinions are of the current PIPA legislation.

Mr. Dahms: Thank you. We represent about 150 different organizations: arts, sports, we have a couple of environmental organizations, a number of human service organizations as well. We haven't actually done any extensive consultation or had focus groups. We've had discussions with our board of directors on this topic. Over the course of time, as was mentioned, the antispam legislation was a major piece of work that we got involved in when that legislation came in, and I think it's a similar discussion about trying to help folks make sense of what's in front of them by way of legislative requirements.

I think our position certainly has evolved from, again, conversations at the board level. I've talked to a number of organizations though not in a formal survey way.

Mr. Carson: Thank you very much. Just one more question here, and I believe it was similar to the one asked to the Calgary Chamber of Voluntary Organizations. I'm just hoping you can also elaborate on how often the collection, retention, or disclosure of information has become an issue within your organization.

Mr. Dahms: Well, it hasn't been raised as an issue per se. I think the tangle comes, as I was mentioning earlier, with organizations being outside the scope of the legislation, and many don't even know that they're in or that they're out. You know, as was mentioned, boards turn over. New people come in. I would expect that if asked, board members of smaller nonprofit organizations wouldn't have a clue as to what they have to be compliant with and what they don't. They just do what they do.

I think the issue really is resident in a lack of knowledge on the part of board members of particularly small organizations but, I think, generally. I think it's fair to say that the people that work in nonprofit service are concerned about the service and not as concerned about all the rules. I think there's an awareness, though, that if there are rules that we are responsible to be accountable for, then we need to know what the rules are and what we need to do to stay on top of them. The point about multiple pieces of privacy legislation, trying to make sense of it all: you know, "Help us," is really what they ask. So I think the issue is really not where groups have gotten into trouble or there have been complaints, because I think common sense has prevailed, fortunately. I think the issue is really in trying, as we go forward, to be clear about: here are the things you're responsible for. And I think simplicity is really key.

11:00

The challenge I would offer is: can we get this right and put it on one piece of paper that says, "Here's what you need to do," and the flip side says, "If you get into trouble, here's how you get out of trouble"? I think that's really the challenge. Let's be elegant in the solution and make it simple, make it helpful. Really, the bottom line here is to protect the privacy of Albertans who are involved in nonprofits: our members, our clients, our customers, our users of facilities. I think the standard of care is really the question. Can we describe the standard of care that we're responsible for and make the way forward a fairly simple and straightforward one?

Again, I'd reiterate, if I could, the comment that the ongoing training and support is really, really important because people do change annually in some of these organizations, and it's really helpful to help people understand what their responsibilities are.

Mr. Carson: Thank you very much.

The Chair: Excellent.

Mr. Gotfried.

Mr. Gotfried: Thank you, Mr. Chair. This is actually a bit of a follow-up question to Mr. Taylor's question to Ms Evans from FCC. Leslie, I know you've got some concerns around how it's going to hinder your volunteers and whatnot. Have you taken a look at how that might translate into costs? I'm sort of assuming here that what you might need to do or want to do is to actually have some additional insurance to cover your directors, to cover volunteers and those sorts of things. Has that been something that

you've looked at at this point in time? Do you actually monetize what this could look like so that you do not have a disincentive for volunteerism and, you know, board participation?

Ms Evans: We have not looked at monetizing it or that. What I would say about insurance is that we have an insurance program in Calgary for all of our community associations and our other members, which range from very small animal not-for-profits up to the Trico family leisure centre. That insurance protects the board against kind of, if you will, stupidity, but it doesn't and can't protect them against gross negligence. So if they wilfully go against – you know, they know this policy is in place or this legislation is in place. They know that they have to comply, and if they don't, their insurance won't step up. They're personally liable. That's the reality of any not-for-profit. We have the best insurance that we can buy as a pool.

Mr. Gotfried: Okay. Thank you.

The Chair: Member Connolly.

Connolly: Yeah. I just have a couple of questions for Mr. Perry and Ms Wong. You mentioned that the collection of personal data is essential for charities. How do you think PIPA assists with this or prevents this collection? Can you share through an example without providing any confidential information?

Mr. Perry: The question is an example of how this act supported or hindered. Most of the time the acts get in the way of being able to share information, but it's based on the interpretation. Say that there are two people in the room: there are at least three interpretations of the law. If there's a nurse and they're treating a patient who is homeless and they're working with a social worker who is working with that homeless individual, there are, in fact, two different databases because the legislation requires that the health information be on its own separate piece and the other one is on another so that they can't even communicate that way. If they're lucky enough that they run into each other or talk to each other, that works very, very well, but then they will fall back to e-mails. Then, of course, there's the concern of sending information over e-mail. So then you have to use unique identifiers, but the two different databases don't have the same unique identifiers. So in assisting somebody who has a health issue and is homeless, all of this stuff just gets in the way.

The legislation is excellent, and it's absolutely required to protect people's information. It just needs to be streamlined so that the best interest of that person is at heart, behind it, and that the professionals who are implementing the work know what they're allowed to do and not allowed to do and know whether they're breaking the rules and know the consequences of breaking the rules and that it's up to them, you know, based on this action, that they need to or not. That's why I like the Children First Act, just because it always puts the primacy of the kid up front there. Like, if the kid is in need, just help them and forget about legislation. That's my interpretation of that.

Connolly: Right.

Just a quick follow-up. If you could just reiterate what changes you would recommend going forward to update PIPA.

Mr. Perry: I think that because we have so many different types of professionals and then you get another argument about whose ethics are higher and that kind of stuff, there needs to be an independent third party that can be asked the question: is this real or not real? I love the suggestions that came up with ongoing training and all those wonderful things and the turnover and all that. They're absolutely correct. But if there is a dispute – and it can't come down to the senior management to dispute because then you get into the politics of an organization – it has to be an independent voice of authority to say what's right and what's wrong on these sorts of things. So the training is required, but there also needs to be in place almost like a very informal adjudicator if that could be put together, an informal adjudicator. I don't know.

Connolly: Perfect. Thank you very much.

The Chair: Excellent.

Mr. Gotfried.

Mr. Gotfried: Yes, Mr. Chairman. Again, I'd like to echo the thanks to all the organizations and representative organizations here. There's no question that the work that's being done in the community by all of you is something that's not only needed but more needed in a tough economy as well.

I'd like to direct a question to Mr. Perry and Ms Wong of CUPS. I know of a lot of the great work that you're doing there. I'm very familiar with your organization. I happened to be in the Mustard Seed, and I know they're going to be opening up a wellness centre soon and that you work with many organizations. Could you maybe give us a sense of the scope of the number of different organizations that you work with in terms of sharing clients back and forth in trying to do the best work that you can do so that we can understand a little bit about the scope of your challenge in dealing with that, putting the clients and patients first and also trying to layer compliance with this potential legislation on the table?

Mr. Perry: We have about 300 different organizations that we work with. Within Alberta Health Services there's a plethora. There are all the different hospitals, the emergency rooms, cardiologists, all sorts of different things, parent education. There's one great program called Best Beginning. They operate within our building. We lease them space at I think it's up to $2 a year now. But it's interesting for them. They can't tell us who's attending the class because of various different legislation. So we can't even go and ask that person: how come you didn't go? Because we don't know, if you know what I mean. They didn't attend the pregnancy class, but – I think that's clear.

We do work with the big shelters, you know, like the Mustard Seed, which is a fantastic organization. We get along with them well. There's the Alpha House drop-in centre. Name the big ones, and we work with them on a regular basis. We actually even have physicians that go out and work in some of these shelters as well. So they'll be within an organization, say Alpha House, and attending to the physical and mental health and doctoring stuff and then be able to communicate properly with the regular staff. There is that face-to-face conversation, absolutely, but for a systemic understanding of how a patient is getting better or not getting better, that's very challenging.

Mr. Gotfried: So it sounds like . . .

Mr. Perry: Did I answer all of that?

Mr. Gotfried: Yeah. It just, I think, demonstrates the breadth of the organizations that you're working with and also the challenges you face in not only dealing with current issues but possibly preventive issues that could be shared with the other organizations.

You also, I know, mentioned the hierarchy of the legislation, and that's obviously of concern. You're dealing with six different acts, it looks like here, and trying to deliver the best possible services. So

that seems to me something that we need to take into account, again, that hierarchy that you mentioned and whether there is any primacy of legislation when it comes to application. I think those comments are very helpful, so I thank you for that.

11:10

Mr. Perry: There's one piece of legislation that if the child is involved with the child and family services, you have to keep the records for 100 years. There are all sorts of weird clauses that appear in and out, and they create more challenge.

In the case of a person who is in recovery from, say, drugs or alcohol and we're not able to properly communicate without an understanding or a good connection with a treatment centre, how are they progressing in their treatment? You don't want to know their case notes or anything like that. Absolutely not. But are they still there? That would be very useful to know. Or if they've abandoned the shop, right? Then we can understand: oh, why did this person show up on our doorstep again? What happened? Not in detail, but it would be good to know.

Mr. Gotfried: Thank you.

The Chair: Mr. Taylor.

Mr. Taylor: Yeah. The question is for Mr. Perry and Ms Wong. You mentioned in your submission that the timeline for giving consent needs to be explicit and that the result of continually asking for consent is that the concept loses validity. Can you expand on what you mean by that?

Mr. Perry: In practice, agencies have different rules. I know some of my colleagues at different agencies keep consent forms for two years. We currently work with a one-year consent piece.

The other aspect of that is that because we aren't able to share information properly with other organizations, we can be asking somebody who comes in four different times for a consent to share and collect information, which gets a little bit annoying for that person to come in and go: one big organization; why can't you get your act together? And then how to retain those records. Where are they destroyed? What are the proper protocols in terms of renewing their consent? So if we're working with a child in our educational areas, we have to go through those each year. You know, there's consent to apply sunscreen, consent to go for a walk, consent to do all these things. So there is this giant signing section that we have every year, and it becomes absolutely meaningless for the participant who is struggling with poverty and trauma and all sorts of different backgrounds, and they go through this meaningless – in my opinion, what they're doing is a meaningless exercise to just get them the help that they require, and then they can go back, hopefully, to their jobs and whatever situations they're living in.

A lot of this stuff is wonderful, and I support it absolutely. It's how to reduce that burden. That's not for my organization. I don't really care about the qualified staff that we have. It is, you know, how to help that individual who is in need of help, that came to our shop looking for it. We need to be able to work together to solve these issues as an organization and as a broader community. But given the limited capacity of the people who are signing these things, and over and over and over again, it gets nowhere.

Mr. Taylor: Thank you.

The Chair: Are there any other questions? On the phones?

All right. With that, I would like to thank our guests for the presentations this morning and for answering the committee's questions. To our presenters: if there is any outstanding feedback or suggestions or comments, please forward them to the committee clerk by September 14.

I would like to note for our guests' information that the transcript from today's meeting will be available on the Assembly's website by the end of the day.

With that, we'll take a five-minute break to allow for the next presenters to join the table here.

Thank you, all, very much.

[The committee adjourned from 11:14 a.m. to 11:22 a.m.]

The Chair: All right. I'd like to call the meeting back to order. The committee is hearing oral presentations today respecting its review of the Personal Information Protection Act. I'd like to welcome our guests on the next panel.

We'll do a quick round of the table to introduce the members and those joining the committee at the table. I'm Graham Sucha. I'm the MLA for Calgary-Shaw and the committee chair, and I will continue to my right.

Mr. Schneider: Dave Schneider, vice-chair and MLA for Little Bow.

Mr. Dach: Lorne Dach, MLA, Edmonton-McClung.

Connolly: Michael Connolly, MLA for Calgary-Hawkwood.

Mr. Coolahan: Craig Coolahan, MLA, Calgary-Klein.

Mrs. Schreiner: Kim Schreiner, MLA, Red Deer-North.

Mr. Carson: Jon Carson, MLA, Edmonton-Meadowlark.

Mr. S. Anderson: Shaye Anderson, MLA, Leduc-Beaumont.

Ms Fitzpatrick: Maria Fitzpatrick, MLA, Lethbridge-East.

Mr. Gotfried: Richard Gotfried, MLA, Calgary-Fish Creek.

Mr. Taylor: Wes Taylor, MLA, Battle River-Wainwright.

Mrs. Szabo: Andrea Szabo, office of Parliamentary Counsel.

Mr. Koenig: I'm Trafton Koenig, a lawyer with the Parliamentary Counsel office.

Dr. Amato: Sarah Amato, research officer.

Dr. Massolin: Good morning. Philip Massolin, manager of research and committee services.

Mr. Roth: Good morning. Aaron Roth, committee clerk.

The Chair: All right. Before we hear from our guests, a quick overview for our guests of the format today. Each group will have 10 minutes to speak, and following all presentations on the panel, I will open the floor to questions from committee members. Please identify yourself before you begin speaking for the record and for the benefit of those listening online.

We'll begin with the first . . .

Ms Jansen: Sorry, Chair. Could you just mention the attendees on the phone?

The Chair: Oh, my apologies. Sorry. And those who are on the phone.

Ms Jansen: Sandra Jansen, Calgary-North West.

Mr. Panda: Prasad Panda, Calgary-Foothills.

Mr. Piquette: Colin Piquette, Athabasca-Sturgeon-Redwater.

Mr. Hunter: Grant Hunter, Cardston-Taber-Warner.

The Chair: Excellent. My apologies to those on the phone.

We will begin with our first presentation, by Service Alberta. The floor is now yours.

Ministry of Service Alberta

Mr. Grant: Thank you, Chair, and good morning. My name is Tim Grant. I'm the Deputy Minister of Service Alberta. With me today on my left I have Cathryn Landreth, recently the ADM for open government; in the seating behind, Joanne Gardiner, who is our PIPA expert; and Manon Plante, who is coming in as the ADM for open government.

As the administrator of Alberta's Personal Information Protection Act, or PIPA, as we refer to it, Service Alberta educates and assists Albertans in understanding PIPA, whether they are individuals or organizations. Service Alberta also assists provincially regulated organizations in ensuring their compliance with the legislation. These responsibilities are primarily accomplished through a direct information line to the public and by providing awareness sessions, online resources, policy interpretation, and general guidance.

As a result of these responsibilities, Service Alberta has technical knowledge as well as an understanding of the privacy landscape in the private sector. This knowledge and experience was drawn upon to prepare Service Alberta's written submission that was provided to this committee in February of this year. The written submission Service Alberta provided was intended to ensure the committee was aware of some important areas for consideration as the committee undertakes this very important review of the act.

Service Alberta also facilitated the co-submission of the department of human resources' information-sharing strategy office. Our colleagues with the information-sharing strategy office are at the forefront of improving service delivery to vulnerable Albertans in partnership with the departments of Education, Health, Justice and Solicitor General, and Seniors and Housing. The information-sharing strategy office deals extensively with the nonprofit sector in its delivery of service on behalf of and in co-ordination with government.

It is not the intent of Service Alberta to direct the committee's consideration of specific issues but, rather, to provide any necessary technical support that would be of benefit to the committee's deliberations. It's an opportunity and benefit for Service Alberta to observe the committee's deliberations in order that Service Alberta may hear and absorb the feedback and considerations informing the committee in its review.

To that end, Service Alberta does not have anything further to add to its written submission and is happy to spend the remainder of the time available answering any questions the committee may have about that submission. Thank you.

The Chair: Excellent. Thank you very much.

We will now move to our next presentation, by the office of the Information and Privacy Commissioner. Go ahead.

Office of the Information and Privacy Commissioner

Ms Clayton: Thank you very much. I am Jill Clayton. I'm the Information and Privacy Commissioner of Alberta, and I appreciate the opportunity to be here to speak with you today. I am joined by my colleagues in the office: Kim Kreutzer Work, who is the director of knowledge management, on my right and, in the gallery behind, Amanda Swanek, who is an adjudicator with my office. I would like to mention that I was just reflecting with Kim and Amanda that all three of us were actually at the table for the first and last review of PIPA, some 10 years ago almost, so we've been working with this legislation for quite a number of years now.

I last spoke to this committee last October, and since that time my office and, of course, numerous stakeholders across the province have had a chance to share our thoughts on how to improve this important piece of legislation. I found that the diversity of submissions was both very interesting and reinforced for me that, by and large, stakeholders recognize the value of PIPA.

I know that you have received my submission, which sets out some ideas, suggestions, and recommendations to strengthen PIPA and ensure that Alberta remains a leader in private-sector privacy legislation across Canada and internationally. I don't intend today to speak to those specific recommendations, but I did want to just provide a little bit of context that may be helpful to you as you deliberate possible amendments going forward.

To start, I just wanted to say a few words about PIPA's substantially similar designation. Most if not all of you are probably already familiar with this concept, but I think that it's important just to keep it front and centre when we're taking a look at PIPA. PIPA is a made-in-Alberta approach to balancing the privacy interests of Albertans with the legitimate need that businesses have to collect and use and disclose personal information. PIPA was purposefully designed to make privacy compliance as simple as possible for small and medium-sized organizations. But I do think it's important to remember that PIPA was not created in a vacuum. There are other global and national forces and principles that shaped how the legislation was initially drafted, how it was previously amended, and how it needs to function in order to be recognized within Canada and internationally.

As many of you will be aware, of course, we have federal private-sector privacy legislation, the Personal Information Protection and Electronic Documents Act, which came into force in 2001 with respect to federally regulated businesses. That legislation, PIPEDA, gave the provinces and territories the option of enacting their own private-sector privacy legislation. If that provincial law was deemed to be substantially similar to the federal law, then the provincial law would operate in that province, and otherwise the federal legislation would apply. Quebec had already passed a private-sector privacy law, and that was deemed to be substantially similar. Of course, Alberta and British Columbia worked very closely to come up with the two PIPAs, which are very, very similar, both of which were introduced in January of 2004 and both of which have been deemed to be substantially similar to the federal legislation and which effectively exempted provincially regulated Alberta organizations from the federal law, PIPEDA, and ensured local oversight by a provincial Privacy Commissioner.

11:30

Of course, Canada's federal privacy legislation, PIPEDA, is deemed to have adequacy status as it relates to European privacy law, and that means that European law recognizes PIPEDA and, by extension, substantially similar laws such as Alberta's PIPA. That means that Canadian businesses have adequate protections for the transfer of personal information within our borders. Without adequacy status, that transfer of personal information for both Canadian and Alberta businesses would be uncertain, and that uncertainty would affect their participation in the global knowledge economy.

I wanted to just draw attention to, certainly, a topic that has been much debated and discussed in various privacy forums across the

country and internationally as of late, and that would be that the European Union recently overhauled its privacy law in the form of the General Data Protection Regulation, which is also known as GDPR. That was approved by the European Parliament in April of this year. Again, remembering that Alberta's PIPA is substantially similar to the federal legislation, which is based on the same principles that European legislation is based on, it's all about information flowing and an ability to do business internationally, nationally, and within the province.

The new GDPR takes the place of the earlier data protection directive, which had been passed in 1995 and required member states to have their own privacy law. Now, for the new GDPR, there's a two-year grace period before the new provisions come into force, so May of 2018, and that will apply to all member states and their citizens.

The GDPR has made privacy law across Europe much stricter than it had been and has enhanced the protection of Europeans' personal information in many areas. It's a massive document. Some of the topics that it takes on are issues around consent and individuals' ability to control their own personal information, how fundamental that is to privacy protection, and around accountability and privacy management frameworks. So there are legislative requirements in the new European legislation, breach notification and around privacy impact assessments. Those are just some examples.

Why does that matter? Again, with the global reach of Canadian- and Alberta-based businesses, not to mention the ubiquity of online activities generally, I think it goes without saying that the GDPR will be affecting how we do business here. I think that looking at some of those amendments that have happened with the GDPR in the European Union, they have the ability to impact what's going to happen in Canada. With the new stricter provisions of the GDPR the adequacy status of Canadian privacy law is certainly being much, much debated right now, and some have said: will adequacy survive the coming into force of the new GDPR, and how should governments and businesses prepare? No one knows at this point what will happen with respect to Canada's adequacy status, and I'm certainly not suggesting that PIPEDA or PIPA will be deemed inadequate by the European Union, but I was reflecting and, in contemplating possible amendments to our own legislation, thinking that we should be mindful of some of these global and national considerations. I have kept that in mind in terms of the recommendations that I made to this committee.

I think that we should be proud of the fact that Alberta – we're already ahead of the curve in many respects. For example, as I mentioned, the new GDPR mandates breach notification, which we've had in Alberta for six years now. In fact, we're the only private-sector jurisdiction in Canada that has those provisions in the legislation, and other jurisdictions like Canada, the federal legislation, and British Columbia are working to catch up with where Alberta is.

In addition, my office did some work with the federal Privacy Commissioner and the Information and Privacy Commissioner of British Columbia. In 2012 we published a guidance document called Getting Accountability Right with a Privacy Management Program, and that document anticipated and is aligned with the new legal requirements in the GDPR around privacy management frameworks. This document that the Canadian jurisdiction has published explains to businesses how they can manifest accountability. Accountability is a basic principle of privacy, to be responsible for the information that you have in your custody or control, but what does that look like on the ground for a business that's trying to implement that?

In harmony with legislative reform in these other jurisdictions, I made a recommendation that this committee have a look at legislating the requirements of a privacy management framework in PIPA. Again, we've done some work to provide voluntary guidance. We've seen the basic principles of that guidance reflected in the European Union. They're now requiring that for legislation to be adequate. We've seen other jurisdictions moving forward to make recommendations for legislative reform to include things like privacy management frameworks and breach reporting.

I think, just to conclude, I would say that in a global economy where private-sector privacy law needs to be substantially similar and adequate and where private-sector businesses are looking for certainty and consistency to the extent that they operate in many jurisdictions, I'm suggesting we need to be mindful when contemplating amendments that could potentially weaken the legislation or carve parts out of the legislation that would be out of step with some of the global and national considerations. I think it's important to remember that although legislative requirements and regulations can sometimes seem to be burdensome, they also help to provide the public business service partners with stability and reassurance that personal information is being protected. I think that is absolutely necessary in today's day and age to actually win and retain customers, so to do business effectively but also to facilitate information sharing.

I'll end my comments there. I'm quite happy to respond to any questions that you have. Again, I'd like to say thank you for the opportunity to be here today. I and certainly my colleagues in the office look forward to being of assistance to you as you continue your work.

The Chair: Thank you very much.

I'll now open the table up for questions by committee members.

Ms Fitzpatrick: First of all, thank you for your submission. Earlier this morning the CCVO mentioned examples of their perception of what a commercial activity would be, and they cited as an example if a group had rented a room or something to another group. In your submission on page 4 you mention that nonprofit organizations must comply with PIPA only when they collect, use, or disclose personal information in connection with a commercial activity. I'm not clear, and I would suspect that many people would have different perceptions of what that means. My question to you is: what do you actually mean by a commercial activity?

Ms Clayton: I'm assuming that you're directing that question to me.

Ms Fitzpatrick: Yes. Sorry.

Ms Clayton: No, that's fine. I think that is a very, very good question. I think you have hit the nail on the head with respect to one of the challenges that we have right now with the way the legislation is drafted and the way that it applies to nonprofit organizations. It's confusing, it's inconsistent, and I think that it gets in the way of information sharing when we actually do need to see information being shared.

For those who might not be aware of how PIPA deals with nonprofit organizations, some organizations that operate on a nonprofit basis are captured by the legislation and some are not. Nonprofit organizations that are incorporated under the Societies Act, the Agricultural Societies Act, or part 9 of the Companies Act are nonprofits for the purposes of PIPA. So if you operate on a nonprofit basis but you don't meet that definition, then you're fully under. But if you do meet that definition, then only the personal information collected, used, and disclosed in connection with a

commercial activity is captured. I go out and speak to nonprofit groups all the time, and I have for years under PIPA, and we spend hours trying to figure out if the nonprofit group meets the definition under PIPA and what is a commercial transaction.

11:40

We have actually issued 14 orders. As some of you will know, we have an informal process, and 92 per cent of what comes through our office under PIPA gets resolved through mediation. A small percentage ends up at the more formal inquiry process. The more formal inquiry process results in a binding order. We've issued 14 orders that have dealt with nonprofit organizations, nine of which involved a determination of whether an activity was a commercial activity. In those orders, for example, we found that running a sports facility that requires drop-in or membership payments was a commercial activity. That's an order that involved Lindsay Park/Talisman. Providing maintenance services for individual homeowners belonging to a homeowners' association: that's a commercial activity. Providing government-funded legal services – this is a recent order involving the Legal Aid Society of Alberta – was found to be a commercial activity. Selling tickets to theatre productions and registrations for theatre programs: also a commercial activity. That's the jurisprudence on what is a commercial activity.

When a matter comes to our office, though, we are looking at the circumstances, the nature of the transaction. It depends, and that's part of the trouble. That's the challenge is that I can't definitively tell you what is and is not a commercial transaction, which leaves nonprofit organizations in a bit of limbo.

Ms Fitzpatrick: So a one-pager is kind of out of the question?

Ms Clayton: We've tried. We've given guidance. We highlight these orders. Anybody can look at the orders. They're on the website. You can look at the analysis. Is it the kind of service that other for-profit organizations are providing? Is there some exchange of consideration which might give it a commercial character? Anyway, we look at the totality of the circumstances, but the challenge is that it's very, very hard to come up with the black and white and say: this is commercial and this is not. We interpret that on a case-by-case basis when it comes to the office.

Ms Fitzpatrick: Okay. Thank you for that response. I see that the representative from CCVO is there and is smiling, so perhaps you've responded as well to her.

Okay. I have a second question. What are some of the typical breach-of-privacy notifications your office receives on a day-to-day basis?

Ms Clayton: Oh. Well, we are receiving an unprecedented number of breach reports from PIPA organizations. I think we've seen an increase every single year. This year in particular we've seen a bump. Well, the year that's just finished. Some of the things that we're seeing more of lately are e-commerce website hacks. I think that has something to do with the amount of online purchasing, that everybody is online retail shopping. So we see a large number of those sorts of e-commerce sites being hacked.

We're seeing ransomware. We've published a couple of breach decisions involving, well, incidents that are associated with ransomware, so either ransomware that truly does lock the information so that the organization can't get at it or stolen information and then ransom demands being made. They're actually two different things. Because of the fact that we get these reported to our office and we look at them quite closely, we're starting to see the nuances, the differences in the types of incidents that take place.

We're also seeing a lot of social engineering and in particular CEO phishing scams. I don't know if you're familiar with that. I was at a conference in eastern Canada not too long ago, and an American speaker there said that this is the number one breach that they're seeing throughout the U.S., affecting millions and millions of people. Basically, what's happening is that somebody, say, in an HR department of a business gets an e-mail that looks like it's coming from the CEO, and it says: send me a list of all the employees and all their social insurance numbers and their driver's licence numbers. The person in HR or the clerk gets very panicky and thinks: I better respond; it's the CEO. They send it to the CEO, and then it turns out it didn't come from the CEO. That's a really common thing. We've published a number of breach decisions just in the last couple of months because, you know, at one point we had six of those in the office, so we wanted to get that out. We're still working, and we're going to get some guidance out around that particular phishing scam. That's very popular.

Snooping. We still see a lot of snooping in databases. Individuals who have legitimate access to a database with sensitive information will abuse their right to access that information. We see that more in the health sector than the private sector, but we do see a fair amount of that in the private sector as well.

Those are probably the trends that I would say that we're noticing right now.

Ms Fitzpatrick: Okay. A follow-up to that one: do you have any authority to report to law enforcement agencies when you have those kinds of breaches?

Ms Clayton: The authority that I have for the breach reports is to make a decision about whether individuals should be notified, so what we do is that we review. Typically the organization is reporting to us, and they're required to report to us what they've done to mitigate harm. Often they have reported to law enforcement, but they're not required to do that. Then I have prohibitions on what I can report without express authority because information that comes to me in the course of me performing my powers and functions as commissioner is confidential.

Ms Fitzpatrick: Okay. Thank you.

The Chair: I'll open it up for members on the phone. Are there any questions? Any other questions from any committee members? Mr. Taylor.

Mr. Taylor: Yeah. Thank you for taking the questions. I was kind of wondering: when it comes down to PIPEDA and yourselves and there's something that could be contradictory, then who takes the lead on that? Right now you're saying that PIPA does have the lead, it sounds like, but is there an order that it would go through to see who actually has control of that?

Ms Clayton: It doesn't exactly work like that. As I said, well, PIPEDA would apply in Alberta the same way it applies in other provinces, not Quebec and not B.C. and not Alberta, but it does apply in the other provinces because those provinces have not enacted their own legislation. Having PIPA effectively ousts the federal jurisdiction within Alberta.

Having said that, many of the organizations that we regulate within Alberta also operate in the other jurisdictions. Think of some of the big box retail stores that operate across Canada. We many, many years ago worked very closely to build relationships with the other private-sector privacy jurisdictions, the federal commissioner's

office, B.C., and Quebec to the extent that they're able to participate. We talk. We talk about cases. We talk about issues. We collaborate on joint guidance documents.

The last thing I want to see is businesses operating in Alberta saying: oh, my God, we have to comply with this, and then it's different in this province, and it's different in this province, and it's different. That sort of thing undermines the legislation and lessens its credibility. This is why we work really hard to harmonize our approach to the legislation, and for the most part I think we've been pretty successful at that.

If there's a matter that affects – I mean, we've jointly investigated various issues with breach notifications. I was just talking about those. They come to our office. They often go to the other offices as well, and we're aware of that. The business tells us that they will let the federal commissioner know or the B.C. commissioner know, if need be, and we have the ability to talk about some of those things due to some amendments that I think were made in 2005. I think it was Bill 8 in 2005. So we do have the ability to share and to talk and to avoid those kinds of conflicts.

Mr. Taylor: Okay. Kind of another question that led from the previous question: with organizations – and you have a lot of organizations that are out there – are there areas or organizations that are in higher noncompliance than other ones, like kind of a general grouping of organizations?

Ms Clayton: I'm looking at Kim here. I don't know if she's got those stats. I know it shifts a little bit, but for the most part I think the organizations you would expect us to hear a lot about or from has remained fairly constant. This is in no particular order because I don't have the actual numbers, so I don't want to say: this one is worse than the other. We have lots of complaints involving retail, but that probably is a reflection of just the number of retail businesses and the kinds of information that they collect. We have lots of complaints and requests for review involving financial corporations. We have a lot of breaches reported by them, too. Again, I think it's a reflection of the kind of, you know, work that they're engaged in and the information that they collect and individuals' expectations of what they are doing with that information. I also think it's a reflection of how diligent they are in terms of protecting information, that they stay in contact with us, they work with us, they talk to us, they report to us because they're sophisticated at privacy compliance.

11:50

So retail for sure, finance, credit, insurance as well, some professional services. But then we've also seen shifts over time. I can remember when, frankly, we had quite a lot of complaints involving lawyers and legal firms. Then we did some education and awareness. Those complaints went down, and they're sort of in and around where everybody else is. Those are probably the main ones, though. Oh, condominium boards and condominium management companies. That's also a big one.

Again, I think that's a reflection of this blending of, you know: there's a business, but there's also home life and friendships and families. You've got me living right next door to somebody who knows all sorts of things about me and my family, and at the same time there's a business relationship where you can't use that information. You have to be aware of the lines that are between the business and the home life.

That's actually consistent with the other jurisdictions. For many years the federal commissioner's office had lots of complaints involving condominium management companies, boards. The same is also true in B.C. We've, all of us, produced guidelines at some point or another to try to, you know, get ahead of that, answer questions before they're asked, get some information out there, and I know that Service Alberta has also done that very same thing, produced guidance for condominium boards.

Mr. Taylor: I'm sure it's very fluid having noncompliance. It's always changing because, you know, the market is always changing, the mentality is always changing. So what do you do to get that information out to them to get compliance from those people?

Ms Clayton: What do we do?

Mr. Taylor: How do you work with industry?

Ms Clayton: We have worked with industry. You know, I'm thinking of a few years ago when we were having a lot of retail complaints. We actually did some focus groups with the Retail Council of Canada to try to identify issues that led to us producing some guidance documents. Particularly at that time it was around photocopying drivers' licences, and then we had a case in the office – I think we have an investigation report publicly about this – about all those photocopied drivers' licences being used to commit identity theft. Somebody was taking that information and then buying stuff with people's stolen identities. We've jointly produced guidance around those kinds of issues.

We watch and monitor to see what the trends are. For example, I mentioned earlier that we're starting to see a trend in breaches reported to us that involve ransomware, so we put out an advisory on our website about how to protect yourself from ransomware. What should you be doing as an organization? I mentioned the CEO phishing scam, so we're working on some guidance around that. We look for those trends.

We look for issues involving – if it's condominium management companies and boards, for example. I remember personally sitting down with Service Alberta reps – this is quite a few years ago – and folks from the north and south condominium associations to talk about what are the issues, what are the answers to some of those issues. That's been available publicly. Then we'll go out and talk to the industry associations. We'll put information on our websites, we'll do presentations at conferences, all that kind of thing.

Mr. Taylor: Okay. Thank you.

The Chair: Any other questions?

Ms Fitzpatrick: I understand also from your submission that there are thousands of active societies under the Societies Act and quite a number of active agricultural societies under the Agricultural Societies Act and nonprofit companies under part 9 of the Companies Act. How do you think PIPA actually applies to them?

Ms Clayton: Well, it may or it may not, first of all, based on how they're incorporated, and it may or may not depending on, you know, what types of commercial activities they're involved in. What I do know is that we do receive complaints about nonprofits. We receive calls from nonprofits asking for assistance and help and "Does the act apply?" and "What should we do?" and "What should we not do?" We seldom have jurisdiction at the end of the day. That's just the truth of the matter.

We have over the years I think answered 20,000 phone calls. We keep track of all the calls that come in. A huge percentage of those calls come from individuals about nonprofits or from folks working with nonprofits asking us questions about how the act applies and if the act applies. Then we get a sense of what issues they're dealing

with. The issues that nonprofits deal with are not any different from the issues that for-profits deal with. They have employment-related issues. They have complaints about use and disclosure of nonprofit information. They use sophisticated information systems. They use sophisticated surveillance systems, biometrics. They have breaches just the same as everybody else has breaches. They have some additional challenges in that a lot of nonprofits have possibly not tremendously sophisticated boards, and often those people are taking records home with them, personal information home with them. It's stored in a garage somewhere. It's stored in someone's basement somewhere. The person no longer is on a board: what happens to that information? Is it still in the basement somewhere? There are those kinds of issues.

I know that there are challenges for lots of nonprofit groups, but there are also lots of resources. We try very, very hard – I know Service Alberta does as well – to assist nonprofits. A lot of them want to comply even if there's no requirement to comply. But I think they've got incredibly sensitive information in many cases. I talk about this a lot, particularly when you're looking at an information-sharing initiative between government and a social service agency. I've said this many a time. Those nonprofit groups are collecting some of the most sensitive personal information about any individual – health information, drug and alcohol information, counselling, victims of domestic violence – very sensitive information, and they want to do the right thing.

From my point of view, why should those clients of those agencies not have the same protections and rights that other individuals do when they're obtaining services from, say, a for-profit organization? They should be able to have a right to access their own information. They should have a right to complain about how their information has been collected, used, or disclosed. They should have a right to an independent review, which is what my office does. They should know that their information has to be protected legally, so the same issues. They have the same issues, sometimes their own unique additional set of issues as the for-profits.

Ms Fitzpatrick: Thank you.

Mr. Grant: If I could just take a minute and add to that. The commissioner, I think, has hit the nail on the head. It really is one of education. There are literally over 10,000 societies in the province. PIPA doesn't apply to all of them in all respects, but the number of organizations that we deal with on a daily basis, trying to determine with them if certain regulations do or do not apply and, if they do apply, how they would be interpreted is a challenge because of the almost patchwork approach to the legislation and multiple pieces of legislation and multiple types of organizations. This is something that, as the commissioner has said, we work with diligently to try and educate Albertans so that they do remain compliant with the acts and with their obligations to maintain individual privacy. It is a challenge, without doubt. It's a great act. The challenge is figuring out if the act applies to you and, if so, how.

Ms Fitzpatrick: Thank you very much. You actually answered my follow-up in that one, too, so thank you.

12:00

The Chair: Excellent.

Mr. Taylor.

Mr. Taylor: Yeah. I just have a quick question. I want you to put perspective on this. With noncompliance from nonprofits and complaints, I guess, perhaps from nonprofits, what is the percentage of those that are coming in? Like, what is the percentage of your issues that are resolved around nonprofits as opposed to the other ones that you have, you know?

Ms Clayton: I don't know if I have exact numbers for you. Oh, I have some stats. Thank you, Kim. Thank you very much.

I have here 67 cases that came in. We had jurisdiction in four, and we had no jurisdiction in 56 of those cases, so about 84 per cent of what comes in to us. It might be a complaint about a nonprofit group, and it turns out that we don't have jurisdiction. In the 15 years that PIPA has been in force, we've had jurisdiction in three complaints involving a nonprofit. So three complaints and one request for review.

Mr. Taylor: Three complaints out of how many?

Ms Clayton: The total cases are 67. We've had jurisdiction in three of those.

If we don't have jurisdiction, we might – you know, commonly we would say that if it was a breach that came in, we would still offer advice on responding to the breach. We would direct them to resources that might be able to assist them. Individuals wouldn't have the ability to follow through the complaint, though. We'd end up shutting the complaint down. We might go to inquiry on a matter if we're trying to figure out if we do have jurisdiction. I previously mentioned we had issued orders in a few cases where we did find commercial activity. Yeah, it looks like, effectively, in most of what comes in involving a nonprofit, we find we do not have jurisdiction.

Mr. Taylor: Okay. Well, thank you.

Ms Clayton: You're welcome.

The Chair: Any other members?

All right. With that, I would like to thank the guests for their presentations this morning and for answering the committee's questions. If there are any outstanding questions or if you wish to provide any additional information, please forward it to the committee clerk by Wednesday, September 14. I would like to note for our guests' information that the transcripts of today's meeting will be available on the Assembly website by the end of the week.

With that, we will adjourn until 12:50. If you could please be back by then, that would be greatly appreciated. Thank you very much.

[The committee adjourned from 12:03 p.m. to 12:50 p.m.]

The Chair: All right. I'll call the meeting back to order. The committee is hearing oral presentations today respecting its review of the Personal Information Protection Act.

I would like to welcome our guests on the next panel. We will do a quick round-table of introductions to introduce members and those joining the committee at the table. I am Graham Sucha, the MLA for Calgary-Shaw and committee chair. I will continue to my right.

Mr. Schneider: I'm Dave Schneider, MLA for Little Bow.

Mr. Dach: Lorne Dach, MLA, Edmonton-McClung.

Connolly: Michael Connolly, MLA for Calgary-Hawkwood.

Mr. Coolahan: Craig Coolahan, MLA for Calgary-Klein.

Mrs. Schreiner: Kim Schreiner, MLA for Red Deer-North.

Mr. Carson: Jon Carson, MLA for Edmonton-Meadowlark.

Mr. S. Anderson: Shaye Anderson. I'm the MLA for Leduc-Beaumont.

Ms Fitzpatrick: Maria Fitzpatrick, MLA for Lethbridge-East.

Mr. Taylor: Wes Taylor, MLA, Battle River-Wainwright.

Mr. Koenig: I'm Trafton Koenig, a lawyer with the Parliamentary Counsel office.

Dr. Amato: Sarah Amato, research officer.

Dr. Massolin: Good afternoon. Philip Massolin, manager of research and committee services.

Mr. Roth: Aaron Roth, committee clerk.

The Chair: Thank you.
Those on the phone?

Mr. Hunter: Grant Hunter, Cardston-Taber-Warner.

Mr. Piquette: Colin Piquette, Athabasca-Sturgeon-Redwater.

The Chair: Okay. Before we hear from our guests, a quick overview of the format of today's meeting. Each group will have 10 minutes to speak, and following all presentations of the panel I will open the floor to questions from committee members. Before you start speaking, please identify yourself for the record and for the benefit of those listening online.

I will first start with Belinda Crowson, past president of the Historical Society of Alberta. The floor is now yours.

Historical Society of Alberta

Ms Crowson: Thank you for inviting me to speak today. My name is Belinda Crowson, and I am the past president of the Historical Society of Alberta, an organization created by the Alberta Legislature in 1907. Our mandate – and forgive me; it's a long one – is to encourage the study of the history of Alberta and Canada; to rescue from oblivion the memories of the original inhabitants, the early missionaries, fur traders, explorers, and settlers of the north and west of Canada; to obtain and preserve narratives in print, manuscript, or otherwise of their travels, adventures, labour, and observations; to secure and preserve objects generally illustrative of the civil, religious, literary, and natural history of the country. As I said, a huge mission, but something we strive to live up to every day.

As such, I actually am here today on behalf of President Collier and all the members of the Historical Society of Alberta and our chapters across the province. On a personal note, I am a public historian and a museum educator who works in and with history every day.

For Albertans to appreciate our history, we must continue to tell the stories of the people, places, and events of our province. But for those stories to be shared in order to inspire people with what has gone before, to showcase the trials and tribulations of our province, to note what we've done wrong so we can do better in the future, to encourage deep thoughts and critical examination of who we are, to make better choices, to create identity and better communities, we need to find the stories before we can even think about telling those stories.

Our publishing arm, the Alberta Records Publications Board, looks for original stories, diaries, journals in order to publish materials that would otherwise not be available to Albertans. It is incumbent on the HSA to provide accurate depictions of the story of Alberta. These stories that we use are in countless documents in private and public hands across the province. We are blessed that so many individuals and organizations in the past preserved these documents that we use today.

However, we not only have to think about the history; we have to think of the future of history. We know our digital world has a danger and that many files will simply disappear. An incredible loss of photographs and documents could occur simply because of how they are stored. We also, though, face the danger of these documents never making it into a future historian's hands because they were deliberately destroyed.

We at the HSA are not experts on PIPA and privacy laws, and we respect that with everything we do, we must balance a person's right to privacy. Indeed, when we publish, we only use private records that are at least 50 years old. But we at the Historical Society of Alberta do know the value of knowing our stories, knowing ourselves. History provides that sense of purpose and sense of place that nothing else can. We can inspire, educate, create a deeper understanding of our present world by history, but we need the documents to tell these stories, and ensuring we have documents from a wide variety of sources means we can tell much better stories that include all the narratives of our communities and our province.

To give you an example of some of the documents, in the Glenbow archives are documents from the Calgary Brewing and Malting Company. One set of documents outlines the hotel system, where the company actually owned or privately financed hotel operations across the province to ensure a market for their beer. The information on who actually owned the hotel, not just who seemed to operate it, has become very useful for research into Alberta's prohibition years. It also, though, provides a sense of how business and industry developed in our province.

In the Mennonite Historical Society of Alberta records there are records from the Canadian Pacific Railway as to which Mennonite settlers purchased land in the Coaldale area, how much they paid for it, and the arrangements made with each farmer related to the acres that were put into sugar beets. This has helped us learn a lot about the Mennonites settling in communities in the 1920s. On a personal note, I also found my great-grandfather's records.

In the Galt archives down in Lethbridge are the records of the Schwartz agencies, originally the colonists' service association, which helped to place central European immigrants on farms and ranches in the Lethbridge area. The company donated many records, but they donated also the specific work placement records, which can be used by people and families studying immigration and by those who want to understand how the agricultural industry developed in southern Alberta.

The research into the sugar beet industry: these records give an insight into the many men who came from central Europe hoping to work one or two years in the beet fields and then either go home wealthy or bring their families over. Unfortunately, they didn't reckon on the Great Depression. Some wouldn't see their families and reunite until after the Second World War; others never did see their families again.

When the Historical Society of Alberta was asked to submit a statement related to the review of PIPA, we wanted to share our concerns about the way the loss of documents can affect the future of history. If records are destroyed when they are no longer of use to a business, how can they become historic documents? Or if the personal information on the documents is rendered nonidentifying, of what use are they to future researchers? Is there some mechanism for ensuring that these documents are kept for archival purposes? What are the provisions to ensure that the appropriate records are maintained? While we have a duty to a person today to protect their privacy, do we not also have a duty to leave an important historic

legacy to future researchers so our story will be better preserved? Is there or could there be a mechanism that helps ensure that future historians have as great an access to records as we have today?

Again, on behalf of the Historical Society of Alberta I thank you for this opportunity to speak with you and to share our concerns.

The Chair: Excellent. Thank you very much.

We will now move to our next presenter.

Canadian Information Processing Society of Alberta

Mr. Olson: Good afternoon. My name is Mark Olson, and I'm a board member of the Canadian Information Processing Society of Alberta. Mr. Sucha, members of the committee, Mr. Roth, I'd like to thank you for your time and attention this afternoon. In our presentation today CIPS Alberta will provide an overview of the relationship between information technology and privacy issues. We will explore how advances in information technology since the inception of Alberta's Personal Information Protection Act will now require new approaches to ensure the continued protection of Albertans' personal information. Finally, we want to offer our expertise and understanding of information technology and the possible ramifications of its use to help in drafting these legislative changes.

Information technology provides enormous efficiencies and capabilities for both our public and private organizations and has made products and services generally available today that just a few years ago would be hard to imagine and that, even if they were, were available to only a few because of the costs involved.

However, information technology also provides the ability to collect and use personal information in ways that while they may advance the interests of the institution or the business involved, they may also reduce or eliminate the control of the individual to determine who holds their personal information or holds knowledge of their personal affairs. Fast and high-capacity systems enable the correlation and combination of data elements to drive new information about individuals. Inexpensive storage has caused us to reach a situation where the retention of data is often less expensive than its effective management and ultimate destruction.

1:00

It was the recognition that the inappropriate application of information technology to the management of personal information could result in the loss of Canadians' privacy that led to federal and provincial privacy protection legislation, including PIPA, being established across Canada. Since the application of information technology is fundamental to the issues of personal data protection, we need to examine how the capacity and application of information technology have changed since these protections came into place.

When PIPA was established in 2003, it was rare for an individual to interact directly with the information systems of an organization. Due to the personnel costs and the high costs of information systems processing and storage nearly 10 years ago, organizations rarely collected personal information beyond what was necessary to complete an individual transaction. Collection and use of personal information was generally restricted to large organizations, and the combination of personal information across business systems was infrequent, primarily due to the high cost of the redundant storage of the information and the development of the software required to correlate personal data across the various systems.

In 2016 the landscape of information technology as it applies to personal information has changed enormously. Today it is not unusual for an individual's interaction with an organization to take place entirely through that organization's information systems. We've all had the frustrations of wanting to deal with a human person and being actively discouraged from doing so. Where this impacts in terms of privacy is that when we as individuals are now doing the data entry and doing the collection, it entirely eliminates the cost friction to the organization to collect personal information.

But the change in terms of information technology that's probably had the biggest impact on privacy is the emergence of tablets, telephones, personal devices that are dedicated to a specific individual, capable of running sophisticated software, and always connected through the Internet to other devices. These devices have hugely increased the volume, currency, and accuracy of personal information that is collected, unfortunately often without direct involvement of the individual.

Our submission provides details of the many ways that changes in information technology have impacted personal information and personal privacy, so I'm not going to bother going in detail through all of these lists. I'd be happy to answer your questions later. Of the various points and what has emerged in terms of personal information, I think the factor that needs to be given the closest consideration is how personal information and its collection, its storage, its correlation have really emerged as a core aspect of the business model of many organizations. This is entirely different than the situation for which the Personal Information Protection Act, PIPA, was conceived, and it will need to be carefully considered when considering what changes are necessary to ensure the continued protection of Albertans' personal information.

CIPS Alberta is not alone in suggesting that the integration of personal information protection with information systems design and operation really needs to be considered as the best way forward for the protection of personal information. CIPS is strongly in support of the concept of privacy by design, which was a concept and a set of practices that was originally developed by Ontario's former Information and Privacy Commissioner Dr. Ann Cavoukian. CIPS Alberta strongly believes that personal information protection needs to become integral to the professional practice of information systems.

In our formal submission, that we provided back in February, we provided a range of responses to the discussion questions. What I'd like to do is highlight just a few of those responses that we think are most relevant to our conversation today.

"Question 16: is the level of transparency required of organizations using third-party service providers outside of Canada sufficient?" One of the founding principles and the strengths of Internet connectivity, which has led to so many changes in our business and personal lives, is that it was designed from the ground up to be entirely independent and agnostic to geographic and political boundaries. While this provides tremendous functionality and opportunities, it is at odds with most individuals' assumptions regarding the use of and the protections for their personal information.

Navigating the complaint-based process of a Privacy Commissioner for a wholly Canadian organization would be a challenge for most Canadians. It is not reasonable to expect the average Canadian to deal with the complexities of a privacy issue when a third-party service provider outside of Canada is involved.

CIPS Alberta suggests that the onus must be placed with organizations that use third-party service providers outside of Canada to communicate clearly to both their potential and existing customers the impact of the protection of their personal information that comes about from the use of such providers. We also suggest that the consent of an individual to have their personal information stored outside of Canada must be explicitly secured. CIPS Alberta

also suggests that the onus is on the organization making use of a third-party service provider outside of Canada to monitor the changes in relevant policies, laws, and regulations and to meaningfully inform those whose personal information they hold when the protection of their personal information has changed.

CIPS Alberta believes there is value to individuals from the enhanced protection of their personal information that comes about when their personal information is managed in Canada by Canadian organizations and service providers. Individuals should be provided with complete information about where their personal information will be managed when deciding which organizations they wish to deal with.

"Question 17: are the provisions of PIPA regarding notification of a breach of privacy appropriate?" CIPS Alberta strongly advocates that when any systems failure, including a breach of privacy, has occurred, full disclosure and support to the impacted individuals to redress the situation are fundamental to the professional practice of information systems. However, the possibility of becoming entangled in a high-profile, legislated disclosure process does act as an inhibitor to individuals to proactively identify actual or potential security issues, and this is counter to what is really good, effective security practice for both large and small organizations.

We would really prefer that all individuals involved with the management of personal information are able to identify to their organization issues or concerns related to the protection of personal information without having to predetermine the consideration of any impacts or outcomes that they may become involved with. We would also suggest that the legislation in terms of breaches is a good practice in terms of dealing when these incidents have occurred, but we do suggest that a purely reactive response to these situations is rarely effective and that we need to begin to explore methods to proactively ensure that effective information systems and personal information protection practices are being employed.

"Question 21: is the application of the act to nonprofit organizations appropriate, or should all nonprofit organizations be subject to PIPA?" Nonprofit organizations . . .

The Chair: I hesitate to interrupt, but we will have time for questions after as well, too.

I will now move to our third presenter, the United Food and Commercial Workers Canada local 401. Please proceed.

United Food and Commercial Workers Local 401

Ms Piechotta: Hi. I'm Katrina Piechotta. I'm in-house counsel for UFCW 401, and with me is Christine McMeckan. She's a senior communications representative with UFCW 401.

I'm assuming everyone has copies of the submission we provided in February. Just in terms of an overview of that submission, UFCW 401 is the largest private-sector union in Alberta. We're probably best known for representing the workers at Safeway and Superstore, but we also represent people that work at JBS Canada; Sofina Foods, which is Lilydale chicken; Maple Leaf; Civeo, which is the camps up north; and Gateway casinos.

Next I discussed some of the sort of absurd outcomes that we currently see from PIPA. I included the example where a prohibited activity right now under the legislation would be someone taking a picture of a park or playground for an organization seeking to protect that park or playground if there are people in the photograph. As we see it right now, in its current form, there are some problems.

1:10

We ran into this back in the early 2000s, when we were involved in a strike at the Palace Casino at West Edmonton Mall. I'm going to get into that in a little bit, but what ultimately happened was that in order to discourage people from crossing our picket line, the union set up a website, www.casinoscabs.ca, and informed people when they were crossing into the casino that they would be able to see themselves on that website. Several people complained to the Privacy Commissioner, and under PIPA as it was at that point the union was found to have breached PIPA.

We didn't feel that this was fair and that it actually breached some fundamental rights the union has with respect to freedom of expression and freedom of association and challenged the legislation on that basis. We were successful at the Court of Queen's Bench level, successful at the Court of Appeal level, and ultimately it went to the Supreme Court of Canada. The Supreme Court determined that PIPA as it was at the time of the Palace Casino strike was unconstitutional on the basis of violating the union's freedom of expression. What happened was that the Supreme Court obliged the government of Alberta to amend PIPA, which ultimately was done in I believe late 2014.

The problem the union has with that at the current time is that it was amended on such narrow grounds as to, in our submission, make it ineffective to protect the kind of freedom of expression that labour unions as well as other organizations should have. Ultimately, what we're looking for is to have PIPA amended to only be applicable to commercial enterprises or to organizations with a commercial interest, and therefore social advocacy groups, labour unions, nonprofit organizations would then be exempt from the legislation. I set this out in the submission as well, but that's actually what they have at the federal level with PIPEDA. There is that exception: only applicable to commercial enterprises.

Now I've gotten way past my index cards. I mean, it's pretty straightforward what UFCW is looking for. Just to sort of give a bigger picture as to what our job is in terms of organizing workers and how we got into the situation where privacy legislation was intersecting with what our role is there, that Palace Casino strike wasn't a strike with respect to wages and benefits and pensions, as the media usually portrays these types of disputes. This was a dispute for a first collective agreement. In Alberta there's no first contract arbitration legislation, so when these workers at the Palace Casino had all voted in favour of joining UFCW and the union was certified, in order for the union to actually represent the members, there needed to be a first collective agreement, and without a legislative mechanism by which to get that first collective agreement, it has to be negotiated. There's actually no impetus on employers to negotiate, and this led to the dispute, and it was one of several first contract disputes that we had over the early 2000s because that was kind of the process, that you have to strike to get a first collective agreement. This strike was about people actually being able to belong to the union, receive the benefit of union representation.

As I said, this was the casino at West Edmonton Mall, with a huge volume of business. There were about 200 employees: lots of new Canadians, lots of individuals speaking English as a second language, some transient workers, young workers, and so on and so forth, the type of workers that most need some extra protection in the workplace in Alberta. They have, you know, the most difficult time in actually achieving that protection given the type of industry that they worked in as well. That's a difficult industry. Sometimes unsavoury things can go on in casinos. You know, you're working as a dealer for minimum wage. You're worried about dealing the wrong hand, that type of thing.

Even when the picket lines first went up, the workers and the union discovered it was more difficult than in traditional dispute circumstances to get people not to cross that picket line. You know, the workers would ask people not to cross. The union would offer rides to people to other casinos. The individuals crossing would say: "No, no. My lucky machine is in that casino. I have to go in that casino. That's the lucky machine."

Ultimately, the union, you know, had a creative strategy in which to express its position in regard to the workplace, and we were limited by the form of PIPA as it was at the time. With the way the amendments currently are, despite the Supreme Court decision, if we were in a similar situation as we were in with respect to Palace Casino, we might end up in the same type of scenario with PIPA as it is, even with the amendments.

That's all I have to say. I don't know if there's time for Ms McMeckan to add anything.

Ms McMeckan: Yes. Thank you. I just wanted to add that documenting people crossing our picket line was something that we did for very important reasons. One is, of course, that it was a security concern. It was a great deterrent for people who were trying to cross our picket line, an excellent deterrent for them to behave themselves at the very, very least. There was a lot of violence on that picket line. People were drinking. We're talking about a casino environment. People come out. They've lost their mortgage payment. They're angry, and they want to take it out on somebody. It was really important for the security.

The other thing, of course, as Katrina has already alluded to, is the educational component of it. Our constitutional right is to exercise lawful union activity, which includes strikes. Not everybody is a fan of strikes, so we get it. We understand the public perception of strikes is a negative one, but it can be a very positive thing in order to encourage an employer, if I could use that word, to finally negotiate fairly. So when we can convince the public to stay away from that picket line, we lessen the risk of violence on that picket line. We also heighten the opportunity for that picket line to be a shorter one. To take away that right from union members, frankly, cuts to the very heart of who we are, what we are, and the service that we provide to the nation in terms of the democratic process.

Ms Piechotta: Thank you.

The Chair: Thank you very much.

I will now open the floor up for questions. Member Connolly.

Connolly: Thank you very much. I'm actually going to start with Ms Crowson if I may. I had a double major in history and political science when I was at the University of Ottawa, so I know there is a lot of difficulty. People always ask: well, how am I supposed to know what is a historical document and what is unimportant? Well, everything is kind of important because you never know what someone might write a paper on. They can be very specific such as sugar beets and even more specific: Hutterites within the sugar beet community in this particular region.

I know that in Calgary the LGBTQ-plus community had a big problem because nobody wanted to house their records for a long, long time, so they're all in Calgary Outlink. They had them in one filing cabinet, and if anything had happened, if there was a flood or anything like that, it would all be gone, and we wouldn't know. Well, we'd know, but we'd only have stories that we can tell. I know that in Ottawa they burned many of the records from residential schools, and that was incredibly hurtful for the historical community.

Quickly, my first question is: do you find any issues or challenges around accessing historical records due to the legislation that is currently in place?

1:20

Ms Crowson: There are always a lot of records you wish weren't shredded. I've done research in a lot of things people deliberately hide. I've written about the red-light district and things like that, so I'm always looking for the records nobody wants you to find. Certainly, there are some of those in place where you can't name people. You can only say: 10 people were prescribed this medication. There are certainly those things there. There are ways around it. Yeah, it's mostly the loss about deliberately hiding things they don't want public that's the hardest part because the records are not there. I think that would be the easiest way to answer that.

Connolly: Right. This is kind of a follow-up. It's very similar. Do you have any issues around censorship while accessing records, and could you provide the committee with a couple of examples?

Ms Crowson: Well, I think we censor ourselves in the historical world because one source could be wrong. So if you can't find it in two or three corroborating sources, then it's not proven or in any way useful. I think there is within the professional historical community a censorship of its own in that you have to be able to prove your sources, back them up, and all those sorts of things. I think that's what we're looking for more than anything. Trust us to do our job well. The documents need to be there, and then there are ethical ways of approaching those documents that exist.

Connolly: Right. Thank you very much.

The Chair: Any other members? Any members on the phone? Mr. Dach.

Mr. Dach: Thank you, Chair. I wanted to turn my attention to the Canadian Information Processing Society for a moment if I might. I have a couple of questions and lines of inquiry. There was a time I remember well, having been a realtor for over 30 years prior to my election, when personal information was collected on paper. I did transmit that information onto a digital form not too many years ago, but in 2016 most organizations no longer rely on paper records of personal information. It's mostly recorded in information systems.

In your submission to the committee you indicated that "in many cases the organization will also hold personally identifiable information that was not disclosed by the individual to the organization, such as data derived from services that track on-line activity or was provided by a social media site," found on page 8. Can you explain how this happens and how this would impact the application of PIPA?

Mr. Olson: It's an enormous challenge to deal with the situation. Many of our online sources are driven by marketing. The revenue source for many of the large services, Google being the most obvious one, is advertising. The value to the advertiser, which directly relates to their fees, comes down to how well they can effectively target the ad to the particular individual. An enormous amount of effort goes into tracking your activity you do online, what websites you looked at, what searches you asked for. If you're just doing that anonymously, if you've never provided anything that identifies you as an individual, there are still some concerns that remain, which we can come back to. But where the challenge comes is where there's some sort of link between the two.

For example, if you've used Google Mail, well, you've now identified yourself to Google, and we are dependent on their honesty and activities and their adherence to the various privacy legislations not to make the connections. At the end of the day, I'm probably not that concerned with Google because they are well aware of the consequences of breaking this situation. I use it only because it's an easy example, but that's where it comes from.

I ran into an interesting situation the other day where I was going into a shopping mall and they had free Wi-Fi. I'm a cheap person. I save my data plan. But to sign up for the Wi-Fi, you had to provide either an e-mail address or your Facebook account. Well, the reason they're asking for that is that it's a way to link your – what they do with those systems is that they track the actual address of your device as you pass through the mall. They know where you are in the mall you're in, which doors you went in, where you went out. If you have innocently provided your e-mail address or your Facebook account, which I'm guessing most people would do without consideration of it, that's where it comes. It's a link somewhere.

The real challenge in managing privacy is that the loss of privacy doesn't come from each individual act. They can be done well, done innocently. It's the correlation across the two that becomes the concern.

Mr. Dach: How fascinating.

I understand that your organization works with information systems professionals in Alberta, and I guess you deal with data management issues a lot. Now, how do you think data management legislation can be given more teeth?

Mr. Olson: Well, I hesitate to try and get into the specifics of it because there are a lot of factors, and we don't have an enormous amount of time on it. I think that I would provide the analogy that we have had a long history of trying to balance the commercial interests with the ethical interests in a whole number of domains. Realty is a perfect example. Why we license realtors is because there's a potential conflict of interest and there's a need to establish standards of ethics and practice and so on. I think what we're suggesting is that maybe it is time to explore something like that in the domain of information technology because while we do have the established regulations, there is no connection to the actual practice.

Mr. Dach: Interesting.

I noted earlier in your submission that you mentioned that destroying personal information actually costs more than retaining it. That was of curiosity to me. Perhaps you might comment on that. I wanted to know what your thoughts are on retaining and destroying personal information, disclosure of private information to a third party, et cetera.

Mr. Olson: Well, I think I'll focus my response on the disposal because it's kind of the simplest case. Disposal of a personal record: it's really a concept from a paper record. Twenty years ago when you dealt with an organization, the paper record was generally the authoritative record, and they may have put the information in an information system, but in general, as we all know, when things went wrong, nothing happened till they went and found the file. That's not the case now with most organizations. The challenge becomes that with most organizations there isn't one massive system that does everything. There will be one system that deals with your interaction over the web. There'll be another system that's dealing with the accounting. There'll be another system that deals with what's called regulation chip management. Then in the back end there are a whole bunch of analytical systems.

As a result, your personal information doesn't just sit in one place; it sits in five or six places within the organization. To say, "Okay; we're done with Mr. Dach as a customer; five years have elapsed; we're going to pull that information," most organizations would be hard-pressed to tell how many copies of it they had, let alone find them all, let alone find all the copies in the mag tape backups that are being run after. Our message is that we have to be very careful on relying on destruction as a control because in most cases it's frankly just cheaper to buy more disk than to implement the data management policies to keep track of it all.

Mr. Dach: Fascinating.

Now, not only is it difficult to know where within an organization your information may be stored, in a multiple number of places, but also it's difficult to know how many countries it may be stored in because of offshore data storage, that we find within a lot of companies. I understand that CIPS is the regulatory authority to assess, approve, and certify information systems practitioners in Alberta, and I'm guessing you hear a lot about data management issues or data tracking issues related to third-party providers. Is there any way that we can strengthen legislation on these third-party providers that are located outside of Canada?

Mr. Olson: I mean, the simple answer from a legislative perspective is no. We're reliant on international organizations. We're relying on the basis of contract law. I think the dimension of it that is worth considering is that CIPS is a member of IFIP, which is the international UN-based organization, and through that there are connections into similar type programs in other countries. That is a solution that may very well be beyond the time and scale that we want to consider, you know, that we can address here in Alberta, but it means that if we want to explore this as a potential solution for Alberta, there is a possibility, certainly, to do it across Canada because we are the Canadian Information Processing Society. There are parallel organizations across Canada, so there's certainly no issue dealing with a service provider in Ontario. There are similar organizations in other countries.

Mr. Dach: Thank you, Mr. Olson.

Thank you, Chair.

The Chair: Mr. Taylor.

1:30

Mr. Taylor: Yes. Thank you, Mr. Chair. Katrina, you had given us some background, which was helpful, with regard to the situation that was happening at the casino. Anyway, that was, like I say, helpful. But given the Supreme Court's decision regarding the right to freedom of expression, should the same exemption be made for employers, and if not, why not?

Ms Piechotta: Well, I mean, the Supreme Court – one level of court, anyway, I think, certainly considered the fact that on these picket lines a lot of times the employers and the union people are recording for exactly the reasons Christine referred to, right? You know, there might be some violence. There might be something that happens that would be used in additional litigation. So I guess in terms of expressing the employer's interest if it's not for – because we're looking for this broad exception, for this legislation to only be applicable in the commercial sense. If it's an employer wanting to communicate its position during a labour dispute, then I guess it would fit under the exemption as well because it wouldn't be necessarily for a commercial purpose.

Mr. Taylor: Okay. So you would be in favour of the employers being able to have that exemption as well?

Ms Piechotta: Well, if you look at the recommendations the union made, we have an example of a potential application provision. It's actually something very simple that we're looking for – right? – which would be that PIPA only applies to commercial endeavours. So because an employer wouldn't be engaged in a commercial endeavour – you know, they would just be engaged in bargaining with their employees – they would fit under that exemption from PIPA. The same would apply to the employer.

Mr. Taylor: Okay. That was more of my question.
Thank you.

The Chair: Mr. S. Anderson.

Mr. S. Anderson: Thank you, Chair. This is directed to the associates from UFCW. I have a union background, so I understand. I'm a steelworker, and I understand exactly, you know, kind of what you guys are saying. Fortunately, I've never been on a strike. I haven't had to. I don't think anybody wants to ever. I understand the reasons why they're there and what they're there for.

Years and years ago my dad was on a line with the Pulp, Paper & Woodworkers of Canada, and some of the stuff he described with recording and pictures was there. There were some things that happened that nobody wanted to happen, you know, and words and some physical things and altercations and things like that. It was recorded on both sides, and I think that because that happened, it brought everybody's aggressions down a little bit because everybody had kind of the same rights in a way. So I know where you guys are coming from with this. You know, freedom of expression and things like that are very big to me as an individual in general but also from my background.

On your recommendations here I just have a few questions, maybe, to get a little more detail, I guess, in a sense. You kind of said a little bit already, but you specified that PIPA should be amended to allow collection and disclosure of information to support freedom of expression. Now, it's kind of a two-parter. How do you think this can be done, and is there actually a specific section in the act to amend?

Ms Piechotta: If you look on page 5 of the union submission, we do provide an example of a potential application provision, so it would be in the application section of the act. As I said, I believe, in my presentation, this is a similar provision that you'd find in the federal legislation.

I just want to note – and I believe the Supreme Court covers it in its decision – that because the Supreme Court has found the Alberta legislation unconstitutional, they give a year for the government to amend the legislation and bring it in line with the Constitution. I believe what would have happened – ultimately, an extension was given as well, so I think 18 months passed before PIPA was actually amended to narrowly fit in what the Supreme Court had instructed.

If there was no legislation in place, I believe Alberta would have reverted to the provisions in PIPEDA because due to some international trade obligations and stuff like that, we need to have privacy legislation in place. Effectively, that's what could have happened, and ultimately that type of exemption is what we'd be looking for in the application provisions of PIPA.

Mr. S. Anderson: Okay. Thank you for that.

I see in your recommendations here where you're pointing to. Yeah, that's kind of what I wanted, just a broader kind of a little explanation, and that's kind of where all my questions are, to get a little more information out of what you've recommended.

One of the other ones that you mentioned was about trade unions and labour organizations, and we discussed about the exemption with the collection, use, and disclosure of personal information for trade union activities. I guess in a sense, I mean, we know a little bit about it. But, like I said, most of my questions here are to ask why you think this is important and to explain a little more. I know from my background, but maybe some other people might not know as much, right?

Ms Piechotta: Well, I guess what I was discussing and what Christine was discussing – and Christine was actually the union rep who was responsible for the Palace Casino picket line. That's why I'm glad she got a chance to talk about that because she was there for all 305 days of that labour dispute. She was there, involved with the employees when they were in the process of applying to be part of a union.

Just in terms of explaining that to the committee, the way you get a union in your workplace is that under the Alberta Labour Relations Code people sign petitions in the workplace indicating that they support a union being a collective bargaining agent on their behalf. In Alberta even if 99 per cent of those employees in that workplace indicated by petition support that they wanted to join the union, there's always going to be a vote. So then there's a vote, and the employees – it's 50 per cent plus one whether they want to join the union or not. Then, of course, the union is only certified, which I think I want to make clear here. This was a strike to get that contract. This wasn't about, you know, doubling your wages or keeping a defined benefits pension or something like that. This was actually to get what's a constitutional right. That is something that's protected in Canada, freedom of association, your ability to belong to a union. This was that for people to exercise that right, they had to go through this entire process of a labour dispute.

Through the course of that, the union needed to be able to exercise – because freedom of association and freedom of expression go hand in hand, right? If you can't communicate why you want to belong to that association or the ideas of that association, you know, what's the point? The Supreme Court, since the Charter has been in place, has consistently recognized that sort of relationship between freedom of association and freedom of expression.

That's where, I guess, the privacy legislation as it was and, our fear is, as it currently exists in amended form would still limit the union's ability to communicate with the public and those workers' ability to convince people not to cross their picket line. That's why we're looking for, I guess, the exemption.

Mr. S. Anderson: Thanks.

1:40

Ms McMeckan: Just to add to that with regard to the second part of your question, our ability to document and get our message out there is critical not just for our members, but it's critical as part of a healthy, functioning democracy. If something in my community is happening like a strike or a lockout, I think that as a citizen I ought to have the right to know about that. Unfortunately, the mainstream media doesn't always pick up on our struggles, depending on what's going on in the news that week. It is not only important to our members, but I think it's an important community service as well.

One of the things that we do as labour organizations is that we do work in communities. We offer, you know, our assistance to different community groups. We are interwoven into the communities. A lot of the people who worked at the casino, for example, or even more so another first-contract battle that we had at Lakeside Packers in Brooks in 2005 – I mean, that was the community. Our ability to communicate and show what's going on

and show people getting run over by buses in Brooks – for example, our president being run off the road by company officials – these sorts of things are really, really key. If we are invested in having a healthy and functioning democracy, they are absolutely key. That's more of a bigger picture perspective if I could offer that.

My view is that corporations are not people and that the Constitution is there to protect individuals and make sure that we have an ability to function in a healthy democracy. So we do believe that our interests are vastly different than those of corporations, and as a result, the court also agreed with us that when we're talking about the balance of power, corporations have a lot of deep pockets and they have almost seemingly endless funds, particularly in the gaming industry. The Constitution is what we end up relying on in order to try to get some counterbalance there to make sure that we do have a functioning and healthy system.

Mr. S. Anderson: Thanks for that. I appreciate that.

You're right about communication. I think it is a big one for me, you know, about getting the right information out regardless of who it is. It doesn't matter if it's employer, union, employees. It doesn't matter. It's a big deal because going on speculation and conjecture and not getting the right information isn't good for anybody.

Ms McMeckan: And that's a very good point. Thank you. I just wanted to say quickly – thank you for pointing that out – that let no one of us ever forget that we still have to be accurate when we put information out there. We are still held to a standard of accuracy. Otherwise, we could be sued. You know, we are always mindful of that. We're not talking about slanderous things. We're talking about reporting with facts and what's going on. That's something that's really key for us as well. It also goes to our legitimacy as an organization who's representing those workers, doesn't it? Right? It really does. If we're out there inflaming the situation with stories and lies or anything like that, obviously we're not going to be taken very seriously.

That's a very good point. Thank you.

Mr. S. Anderson: Great. Thanks.

That's all I've got, Chair.

The Chair: Mr. Gotfried.

Mr. Gotfried: Thank you, Mr. Chair. It's maybe directed towards Katrina, the question here. I don't know the specifics on it, but I know that there are some instances where employers have also wanted to communicate with members of the public or members of an employee group, and I think there's an example of AHS doing that. Again, it sounds to me like you're advocating for openness on both sides, that both the unions and employee groups can communicate clearly, again, without inflammation, on information relating to labour issues and things like that. Would that be a correct interpretation of what you're saying?

Ms Piechotta: Well, again, I think that's in this sort of model provision that the union has set out here. You know, the act applies to every organization in respect of all information that the organization collects, uses, or discloses in the course of commercial activities. So if you don't fit under that broad umbrella of commercial activities, then the provisions in PIPA wouldn't apply to you.

Again, I mean, I'm a union lawyer. I do grievance arbitration 99 per cent of the time. I'm like a criminal defence lawyer if you get in trouble at work. So I'm not a privacy expert, but as I think we see it, communication in the course of a dispute wouldn't fit under that commercial activities umbrella for either party.

Mr. Gotfried: Okay. So you're advocating, really, for a balance of rights within this part of the privacy act?

Ms Piechotta: Yes. I think labour relations typically, even in Alberta, tries to be a balance. You know, we would submit that it does not that great a job of balancing interests, but I think that if you even look at the Labour Relations Code, it does try to protect both employer interests and union interests and kind of balance that. Actually, the whole basis of labour relations is that balancing.

Mr. Gotfried: Okay. Thank you.

The Chair: Any other questions?

Mr. Schneider: Mr. Olson, in question 5.5 of the submission it was asked, "Does PIPA adequately support individuals who are unable to provide consent?" You had talked about, in the second paragraph of your response, revoking section 61(1)(b) and amending 61(1)(c). Could you expand on that a little bit for me, please?

Mr. Olson: Sorry. That was . . .

Mr. Schneider: Question 5.5. I guess that is what it was.

Mr. Olson: I think it comes to a general question, you know: the foundation of all of our privacy legislation is consent. The comment was made earlier today in terms of CUPS that it becomes so common that it becomes kind of a meaningless exercise. We are concerned where there is any context where a minor can issue consent. We really question how valid that is, and we would like to see that strengthened, that basically minors cannot provide consent and, from extension to that, very strict protections in terms of the use of personal information of minors. Does that answer the question?

Mr. Schneider: Do you believe that minors are actually giving consent in cases?

Mr. Olson: Well, I mean, the system may . . .

Mr. Schneider: Well, I guess you can be anything on the Internet, right?

Mr. Olson: It's like the old *New Yorker* cartoon, "On the Internet, nobody knows you're a dog," and so on.

Sorry. I'm trying to recall a lot of things that we do. I think that basically what we're saying is that there should never be an assumption of consent on the part of individuals. I think it is a fair question in many cases. You know, in most cases consent in terms of personal information is buried within a terms-of-use agreement on a website or a service and so on. I'm seeing the nods. We all know how thoroughly we have read the terms-of-use agreements and so on. When a minor goes in saying, "They've got a game I want," there's a 16-page terms-of-use agreement which includes consent to personal information. The point of topic we have at the moment is the use of personal information, and we do not feel that there should be under any context the use of a minor's personal information buried within there.

Mr. Schneider: Okay.

The Chair: Excellent. All right. With that, I hesitate to interrupt, but to allow us to stay within our timelines, we will adjourn for about 10 minutes.

First, I want to thank our guests for their presentations this afternoon and for answering the committee's questions. If a question

is outstanding or if you wish to provide additional information, please forward it through the committee clerk by Wednesday, September 14. I would like to note for the guests' information that the transcript of today's meeting will be available via the Assembly's website by the end of this week as well.

With that, we'll take a 10-minute break while we prepare for the next presentations.

[The committee adjourned from 1:49 p.m. to 1:59 p.m.]

The Chair: All right. With that, I'll call the committee back to order. The committee is hearing oral presentations today respecting its review of the Personal Information Protection Act, and I would like to welcome our guests on the next panel.

Before we commence this panel, I would like to note for the record that the Public Interest Advocacy Centre was contacted in regard to making a presentation but indicated they were unavailable today. If committee members have any follow-up questions specifically for this organization, please send them after today's meeting to the committee clerk, who will send them to the Public Interest Advocacy Centre on the committee's behalf.

We will do a quick round of the table to introduce members who are joining us at the table. I'll start to my right.

Mr. Schneider: Dave Schneider, MLA, Little Bow.

Connolly: Michael Connolly, MLA for Calgary-Hawkwood.

Mr. Coolahan: Craig Coolahan, MLA for Calgary-Klein.

Mrs. Schreiner: Kim Schreiner, MLA for Red Deer-North.

Mr. Carson: Jon Carson, MLA for Edmonton-Meadowlark.

Mr. S. Anderson: I'm Shaye Anderson. I'm the MLA for Leduc-Beaumont.

Ms Fitzpatrick: Maria Fitzpatrick, MLA, Lethbridge-East.

Mr. Gotfried: Richard Gotfried, MLA, Calgary-Fish Creek.

Mr. Taylor: Wes Taylor, MLA, Battle River-Wainwright.

Mr. Koenig: Trafton Koenig, Parliamentary Counsel with the Legislative Assembly Office.

Dr. Amato: Sarah Amato, research officer.

Dr. Massolin: Good afternoon. Philip Massolin, manager of research and committee services.

Mr. Roth: Aaron Roth, committee clerk.

The Chair: I am Graham Sucha, MLA for Calgary-Shaw and committee chair.

Those who are on the phone.

Ms Jansen: Sandra Jansen, Calgary-North West.

Mr. Dach: Lorne Dach, MLA, Edmonton-McClung.

Mr. Piquette: Colin Piquette, Athabasca-Sturgeon-Redwater.

The Chair: All right. Before we hear from our guests, a quick overview of the format of today's meeting. Each group will have 10 minutes to speak. Following all presentations on the panel, I will open the floor to questions from committee members. Please identify yourself before you begin speaking for the record and for the benefit of those listening online.

We will first proceed with the Insurance Bureau of Canada.

Insurance Bureau of Canada

Mr. Lingard: Thank you, Mr. Chair. I am Steven Lingard, assistant general counsel and chief privacy officer at the Insurance Bureau of Canada. I'm appearing here today on behalf of my colleague Bill Adams, who is IBC's regional vice-president in Edmonton. Mr. Adams had planned on attending here today, but he was called away to a matter in northern Alberta. He sends his regrets to the committee members.

IBC is a national industry association and represents more than 90 per cent of private home, car, and business insurers in Canada. The property and casualty, or P and C, insurance industry also works to improve the quality of life in communities by promoting loss prevention, safer roads, crime prevention, improved building codes, and co-ordinated preparations for coping with natural disasters. IBC and its members have been particularly involved in helping rebuild communities in the regional municipality of Wood Buffalo following the Fort McMurray and area wildfires.

I appreciate the opportunity to speak with you today about the importance of ensuring the protection of privacy for Albertans while allowing companies the flexibility to develop new and improved insurance products to meet the needs of Alberta consumers. IBC has actively participated in discussions with the Alberta government on the Personal Information Protection Act, or PIPA, from the early days, when PIPA was being drafted, to the first PIPA review in 2006 and then the statutory reviews, including this comprehensive review.

P and C insurers understand the importance of protecting the personal information of their customers and insurance claimants, and they take this obligation very seriously. Insurance products change, and new products are developed to meet the changing needs of consumers. In IBC's view, the protection of personal information can best be achieved through a collaborative approach between individuals, industry, and government.

IBC filed a written submission on February 26 on the current PIPA review. As we say in our submission, IBC believes that PIPA largely remains both relevant and responsive to the privacy needs of the insurers that operate in Alberta and Albertans. However, we have identified some areas in which PIPA can be improved. For example, we do not believe that given the increasingly global nature of business there is a need for the PIPA provisions regarding transparency for the use of third-party service providers.

These provisions were added after the 2006 review, when the protection of privacy for outsourced services was relatively new. However, since then it has become a modern business reality. At that time there was a concern that information sent outside of Alberta or Canada would not be covered by any recognized privacy law and that individuals would lose all control of their information. However, the fact remains, then and now, that if the information is collected by the organization in Alberta, that organization is legally obligated to ensure that the information is protected in accordance with Alberta law.

2:05

This obligation can be fulfilled through a strict, well-worded third-party service provider agreement that specifically sets out the privacy responsibilities of the service provider and the ability of the organization to enforce these responsibilities. As well, most P and C insurers are regulated by the federal Office of the Superintendent

of Financial Institutions Canada, or OSFI, as its acronym is. In 2003 OSFI issued guideline B-10, outsourcing of business activities, functions, and processes. Then in 2012 OSFI issued a memorandum on new technology-based outsourcing arrangements. The guideline sets out detailed requirements that an organization's management and board of directors must follow for all outsourcing arrangements. These guidelines require a high level of diligence for outsourcing.

Another area of PIPA that we believe needs further discussion is the mandatory reporting and notification requirements for breaches of privacy. The Alberta PIPA, not to be confused with the B.C. PIPA, was the first general private-sector privacy law in Canada to require mandatory breach reporting. In Alberta a breach of privacy must be reported to the Alberta Information and Privacy Commissioner. The commissioner then determines whether the organization needs to notify affected individuals.

In contrast, the federal Personal Information Protection and Electronic Documents Act, or PIPEDA, was recently revised to require mandatory reporting of data breaches to the federal Privacy Commissioner and mandatory notification to the affected individuals as well as other organizations all at the same time. So there are now two different models reporting data breaches, the Alberta model and the federal model. Many businesses operate across Canada, and it would be a real benefit to citizens and organizations alike if there was one consistent requirement for breach reporting.

The final item that I would like to include in my comments is in regard to exceptions to consent. PIPA currently has a limited number of exceptions where personal information can be collected, used, or disclosed without the individual's consent. We understand the need to restrict the number and scope of these exceptions, but we are suggesting the addition of an exception where the personal information is contained in a witness statement and its collection, use, or disclosure is necessary to assess, process, or settle an insurance claim. The issue here is the fact that a witness statement contains information about both the witness and the person who is the subject of the witness statement. It is important for the settlement of insurance claims that an insurer is able to rely upon a witness statement.

I would like to note that similar exceptions are in the federal privacy law, PIPEDA. As well, the B.C. Legislative Assembly special committee that reviewed the B.C. PIPA in 2004 and 2015 has also included this recommendation in its report to the B.C. Legislative Assembly. So this exception is currently in the federal law, and it's also being proposed in the B.C. law.

I'd like to end my presentation today, my very brief comments, by reiterating our key message. In our view, PIPA is comprehensive in scope and provides privacy protection to the citizens of Alberta, and apart from some minor changes as set out in our submission, we do not believe that it requires any major revisions. I'd like to thank the committee for this opportunity to speak with you today, and I'd be pleased to take any questions that you may have about my comments or our written submission.

Thank you very much.

The Chair: Excellent. Thank you.

We will now move forward with the Canadian Marketing Association. Please proceed.

Canadian Marketing Association

Mr. Hill: Thank you, Mr. Chairman, and thanks to the committee for the invitation to appear before you today. This is further to our submission to the committee earlier in the year. Also, thank you to your clerk and support team for making the arrangements for us to appear by video conference. We very much appreciate the work that they did to allow this to happen.

My name is Wally Hill. I am the vice-president of government and consumer affairs for the Canadian Marketing Association and also the association's chief privacy officer. Joining me this afternoon from Ottawa is David Elder, the CMA's special digital privacy counsel from the firm of Stikeman Elliott.

The Canadian Marketing Association, or CMA, is the largest marketing association in Canada and is the national voice for the Canadian marketing community. Our advocacy efforts aim to promote an environment in which ethical marketing prevails in communicating with and serving consumers. Further to our submission earlier in the year, today we would like to focus on two specific areas, the notification of a breach of privacy and forms of consent and the conditions attached to their use.

Notification of a breach of privacy. In that area the CMA supports the existing rules and processes of PIPA for reporting a breach of personal information. Those rules are working well in protecting consumers. Organizations have also become accustomed to the rules and have been responding well. Unless there is a compelling need for change, we believe that the rules should remain the same. Any amendments that might be proposed should be based on a compelling reason for change and should not be taken lightly given that organizations would need to invest significant resources in retraining employees and altering policies, procedures, and established reporting techniques.

The concept of a real risk of significant harm remains at the core of PIPA's breach requirements, and it's important that this be defined but flexible enough for the Privacy Commissioner and organizations to assess whether each breach situation presents a real risk of harm. This ensures that notifications do not become excessive and routine and thereby create the risk of notification fatigue, where consumers stop paying attention because they're receiving too many notices involving minor incidents.

PIPA should also continue to reflect that breach notification to individuals can be either direct or indirect. While an incident should be reported to an affected individual directly for the most part and usually, in some circumstances it may not be appropriate or possible even for an organization to do so; for example, where direct notification could increase the risk of harm to an individual or where limited or incorrect contact information might mean that many notices would not be received or even where there are a very large number of individuals affected by the breach such that the notice might be impractical for the organization involved. In those cases, it may be more appropriate to provide for indirect notification, and PIPA provides for that possibility.

The CMA notes that where notification to the commissioner is required, the law prescribes that such notification be in a form and manner detailed in the regulations. While these forms in other jurisdictions in Canada, including B.C. and the federal jurisdiction, are similar, they're not identical, and each form has to be completed separately by affected organizations. Where an organization is faced with a breach of national proportions, the organization's time and energy should really be focused on containing and remedying the breach and, where appropriate, notifying affected individuals as soon as practical.

It would be of great benefit to such organizations if data breach reporting obligations could be streamlined through the development of a standard breach reporting form for all Canadian jurisdictions. In that regard, the CMA urges the government of Alberta and the office of the Information and Privacy Commissioner in Alberta to

work with federal and provincial peers to develop a standard reporting form.

On the issue of consent the CMA is of the view that the current provisions relating to consent are well crafted and provide for sufficient flexibility to recognize a variety of legitimate approaches to doing business. That flexibility should be maintained in the law. The CMA generally agrees that "an organization cannot require an individual to consent to the collection, use or disclosure of personal information as a condition of supplying a service or product, beyond what is necessary to provide the product or service." That's a quote from your discussion paper and, I believe, from the law. However, there are a number of situations where such exceptions to that rule may be warranted. A consumer may be legitimately required as a condition of providing a good or service to provide additional personal information beyond what may seem as immediately necessary to deliver the good or service in question.

2:15

In today's economy many goods and services are offered on terms where the consumer pays only a portion of the true price of the goods or services and in some cases pays nothing at all. For example, many online services and apps are provided free of charge to users but depend entirely on advertising and increasing the interest-based advertising in order to support the service. In addition, discounted prices may be provided in some cases in exchange for the ability to collect and analyze consumer data to better understand consumer needs, market trends, and to be able to better design and deliver products and services.

CMA submits that business models where the use of personal information is central to the fundamental exchange between the parties are entirely legitimate and need to be contemplated and provided for by PIPA. PIPA must recognize legitimate circumstances in which individuals may not be able to obtain certain goods and services without agreeing to their personal information being used for advertising or other purposes that some might incorrectly characterize as secondary to the initial transaction.

CMA notes that this principle has been recognized by other regulators. For example, Facebook case summary 2009-008 from the office of the Privacy Commissioner of Canada concluded that advertising is essential to the provision of the service offered by Facebook and that persons who wish to use the service must be willing to receive a certain amount of advertising.

With respect to the adequacy of forms of consent currently provided in PIPA, CMA considers that the current framework works very well. In particular, CMA would like to underline the importance of the act's recognition of the range of approaches to consent, ranging from deemed consent to implied consent to other nonexpress forms like consent by not opting out to express forms of consent like opt-in or double opt-in. That said, in the commercial environment organizations should be able to rely on the understanding that individuals will opt out themselves if they object to the collection, use, and disclosure of their information. While acknowledging that the use of opt-out consent should generally be limited to nonsensitive information, CMA strongly supports the continued recognition of the validity of opt-out consent as being a form of consent that is vital to consumer-friendly commerce.

More explicit forms of consent can result in annoyance to consumers in the context of many routine commercial transactions and could therefore lead to greater frustration and fewer completed transactions. Ultimately, organizations should be encouraged to come up with an architecture that works best in a given environment with the understanding that proper notice to consumers is crucial and that consent should be expressed in an appropriate form, depending on the nature of the information, the context, and the reasonable expectations of consumers. Users, in turn, should be confident that organizations will be held accountable for following correct privacy practices and for protecting consumers' information.

In closing, CMA would like to stress the key elements of flexibility that are there in PIPA and the collaborative operating model of PIPA, that has been highly effective and resulted in a high level of voluntary compliance from Canadian businesses. Additionally, PIPA permits the . . .

The Chair: I hesitate to interrupt, but the allotted 10 minutes has concluded.

We will now open it up for questions. On the line I have Mr. Piquette, who has a question. Go ahead, Mr. Piquette.

Mr. Piquette: Yeah. Sorry for the delay. It took a while to get unmuted.

Actually, I have a few questions. I guess I could take the one and, with the chair's permission, any after that. My question is regarding the presentation by the Insurance Bureau of Canada. I guess quickly, before I get to the question, I would like to take the opportunity to thank and congratulate IBC for the excellent outreach they did during the Fort McMurray fire. I know that it made a big difference to a lot of scared and confused policyholders. I think your quotes people did an excellent job and that in general the industry cleared itself very well and went above and beyond many times what would have been reasonably expected.

I should also in full disclosure, before asking the question, say that I am a former insurance agent myself, a former representative of the Co-operators insurance. I kind of have a bit of an understanding of some of the concerns that are embodied in the IBC's presentation. However, that doesn't mean that I don't have a few questions as well.

My first question is in regard to the IBC response to question 8 on page 3 of your submission regarding the suggestion to provide transparency reports on disclosure to law enforcement and public agencies. I guess the first point is that I've had to deal with a few of those in my own career over the years, so I'm not sure how rare these really are nor how IBC could determine that since at present there is no reporting requirement. Insurance companies collect a large degree of very sensitive personal information in the course of providing service and policies, and I'm not sure if it's unreasonable for the public at large to have an idea of just when and how this information is being shared.

I'm also uncertain how this could be considered an unduly onerous requirement. My presumption is that agents have been faced with these types of requests by their various compliance departments and that therefore the compliance departments should be easily able to provide these records. If they don't do that, they probably should. I guess: how is this going to be onerous? And finally, how would that actually, in your opinion, have a chilling effect on what information is disclosed?

Mr. Lingard: Okay. Thank you very much. I appreciate your questions. The first part about the number of situations when this would come into play. Question 8 is, "Should organizations be required to publish transparency reports on disclosures made without consent to public bodies and law enforcement agencies?" As you know, Mr. Piquette, it's standard practice within the industry when law enforcement contacts an insurer and asks for information for the insurer for the brokers to say: "Thank you very much for your phone call, but, please, at the very least, you need to

send me something in writing. You need to show us your authority, the authorization under which you are requesting information." Increasingly we're asking law enforcement to go and get a warrant so that it's not disclosure without consent; it's disclosure pursuant to a legal requirement.

That situation is not happening as much as it did with the telcos, and I think that was the situation that raised the most issues, where law enforcement did go to the telecommunication companies and ask for large amounts of information. With insurers the requests are less frequent. We know from checking with our members that they don't get that many requests from law enforcement but that they do from time to time. We ensure that there are no fishing expeditions, that the law enforcement provides their authority or gets a legal warrant.

The other question you had, about it proving to be onerous. P and C insurers and brokers are heavily regulated to start with. They're regulated at the provincial level. The Alberta superintendent of insurance regulates for market conduct. The federal superintendent regulates for most insurers on solvency and capital. We have the privacy commissioners, provincial and federal. You keep adding layer upon layer of regulation. What might seem to be, well, just one more piece of information, one more form for a compliance person to fill out: at some point it just adds up and it adds up and it adds up.

In our situation we don't think that there are very many situations where these disclosures are being made without consent to public bodies and law enforcement agencies, so we don't see for our industry the need to address this issue because it's not an issue. Any additional requirement is excessive, in our view.

I hope I've been able to answer your question, Mr. Piquette.

2:25

Mr. Piquette: Well, I mean, I guess it sort of goes back – I'm not sure. I guess I have to take your word that it isn't an issue, but thank you.

Do I have the chair's leave to ask another question?

The Chair: Yeah. You can do one supplemental.

Mr. Piquette: Okay. I just had a question referring to page 3 of your submission, asking for a new exemption to be introduced into section 24(2) of PIPA to enable an insurer particularly to "refuse an individual's access to their own personal information." Now, in the submission I see that that could "compromise the accuracy and availability of the information or . . . jeopardize the process." It's the claims process that we're referring to. I just wonder if you could elaborate on that a bit for the committee, why this exemption would be important and how the lack could compromise information, as I'd stated.

Mr. Lingard: Well, this would be in a situation where a claim is currently being handled. The individual puts in a request for information. In some situations there may be a person who's making a fraudulent claim or is trying to bend the rules, so if they can get access to the information about them in the file, they can then either change the facts or change the information they're providing to the insurer. In a claims-handling situation it can become an adversarial process. We have to remember that the claims-handling process can involve either the insurer and its own policyholder, a first-party claim, or it can be a claim by a third party, someone who's not a customer of the insurer. They've made a claim, and that can be an adversarial type of claim. It's to protect the information that's in the insurer's file that's necessary to thoroughly and properly investigate the claim, to settle it properly. But for someone to get access to that information while the claim is being examined can lead to an abuse of the process. So that's what our concern is.

Did that answer your question, Mr. Piquette?

Mr. Piquette: Yeah, it does. Thank you.

The Chair: Excellent.

I'll open up the floor. Any other questions? Mrs. Schreiner.

Mrs. Schreiner: Thank you, Mr. Chair. My questions this afternoon are for the Canadian Marketing Association, so to Mr. Hill or Mr. Elder. At the end of the day my main concern is that the personal information of Albertans is not being used for purposes not consented to. Given the interconnectedness of people and services in a global economy, as you noted, how can we ensure Albertans' interests are protected and third-party services remain accountable?

Mr. Hill: Thank you for your question. I think the answer lies in a privacy legislative framework like PIPA that applies a strong accountability obligation on the part of businesses and marketers to both notify consumers when they're using their information and how they're going to be using it and imposes on them also the requirement to obtain consent as well as, you know, to adhere to all of the other principles that are built into the act as security for information and ongoing accountability. I think that is how as legislators you are able to ensure that Albertans' personal information is protected, by having a robust but also a flexible, realistic legislative framework, that businesses can in fact comply with, and working with a Privacy Commissioner to ensure that consumers' personal information is protected.

David, I don't know if you've got anything to add specifically.

Mr. Elder: Yeah. I guess I would just underline the point that under the accountability principle, for the organization that's initially collecting the information, if they happen to share it with or outsource to another entity in another country, that organization that initially collected the information continues to be responsible for it at law. We've seen a number of cases where Privacy Commissioners have taken those organizations to task for not, you know, having sufficient controls to protect that information and keep it out of harm's way. So there's a built-in mechanism in the law today and a very strong incentive for companies to take those additional steps when outsourcing.

Mrs. Schreiner: Thank you.

To the association again, to Mr. Hill or Mr. Elder. Thank you for your submission. Your submission recommended that PIPA should be flexible and allow organizations to use individuals' information, that you talked about, as a condition of service. You specifically mentioned that information may be used for advertising and personalizing services but also noted that it should not be limited to this. Do you feel that this could potentially leave a grey area open?

Mr. Hill: It's very hard to predict, you know, in the fast-changing, fast-moving economy that we are living in today and operating in, what sort of uses of personal information may become possible as we go forward. What we were really addressing in that part of our submission was to make the point that, contrary to some traditional business models, in the online economy many goods and services are offered to consumers free of charge in exchange for the use of information. It is the use of their personal information that enables, economically, the platform that the consumer is benefiting from.

So it's extremely important that any organization operating in this space be completely forthright in advising consumers, providing the notice that PIPA sets out as an obligation, regarding the information that is being collected: what information is being collected, how it is being used. But there are some cases where the need to collect and use that information is sort of part of the exchange, the commercial exchange, that is going on.

It may appear that the collection and use of that information for other advertising purposes, for example, or some other use is not absolutely essential to the provision of the service, but the reality is that it is what is paying for the service that's being provided to the consumer. In those situations, while notice is extremely important, as it is in all cases, it is possible that you have an organization saying: "No. To use our platform or to use our app online, this is the information that we require of you. If you don't want to provide that information to us, that's fine, but you won't be able to use the application because this is how we sustain it."

That understanding is not always going to be the case, and it's not always going to be able to be justified, but it was recognized in the Facebook finding of the federal Privacy Commissioner, that I mentioned, that there are instances where that kind of exchange is justified.

Mr. Elder: If I could just add to that. Back to your question, to the extent that there is ever a grey area, I think this highlights the role of the Information and Privacy Commissioner. So while there may be some inherent flexibility within the statute itself, which I think is a good thing, it is also the role of the Information and Privacy Commissioner to turn what might look like it's grey into black and white either through issuing guidance or findings in particular cases. Over time we get a very clear idea of what the boundaries are and what is permitted and what is not.

2:35

Mrs. Schreiner: Thank you, Mr. Hill, Mr. Elder.

The Chair: Are there any other questions? Any members on the phone?

Mrs. Schreiner: I actually have another question, again to the Canadian Marketing Association. In your submission you noted that it is common practice for many organizations to notify individuals that their personal information may be transferred. My first question is: in what format does this notification take place? I know that many services ask you for your consent, but this may be after pages of fine print listed in the terms and conditions. What I'm getting at is: are we sure that individuals are aware that their information may be sent to another jurisdiction, and how can we make sure that they are aware of this?

Mr. Hill: David, I'm going to allow you to answer this one. You're closer to the crafting of some privacy policies.

Mr. Elder: Sure. To your point, Mrs. Schreiner, yeah, it is typically in a privacy policy that an organization would notify individuals about storage or processing outside of the country. I think, you know, privacy policies are improving over time. There is certainly a bit of an ongoing challenge. There's a lot of information that needs to be imparted to affected individuals that the law requires that you need consent for. I think organizations increasingly are moving away from some of the really long form privacy policies that we saw in the very early days to more creative or innovative approaches.

Often you'll see the layered approaches to privacy policies, where you'll have Q and As or short summaries of the policy and a number of tools so that people can get the information they want when they want it. If someone is about to use a service and is particularly concerned about their data being stored or processed outside the country, there are increasingly tools available. They can go right to an FAQ, for example, and get that answer. There are certainly some challenges in trying to communicate all of the elements of a privacy policy, including this, but I think organizations are increasingly rising to that challenge, aided quite a bit by technology.

Mrs. Schreiner: Thank you, Mr. Elder.

The Chair: Thank you.

Are there any other questions from the floor? On the phone?

With that, I would like to thank our guests for their presentations this afternoon and for answering the committee's questions. If there's a question that is outstanding or you wish to provide any additional information, please forward it to the committee clerk by Wednesday, September 14. I'd also like to note for our guests' information that the transcripts of today's meeting will be available via the Assembly's website by the end of this week as well.

Thank you, all, very much.

Mr. Hill: Thank you.

Mr. Elder: Thank you.

Mr. Lingard: Thank you very much.

The Chair: Hon. members, in preparation for the deliberation phase of our review of the Personal Information Protection Act, it is practice for the committee to request the assistance of research services in preparation of a document summarizing the issues and proposals identified throughout the consultation phase.

Before I proceed, I'm going to open it up to research services to provide us some more information.

Dr. Massolin: Thank you, Mr. Chair, for this opportunity. I just wanted to take a moment or two to explain to the committee what this document is. As I look around the table, I see that many of the members have maybe already encountered one of our research issue and proposal documents. What that is is basically a summary of the salient issues and proposals that have come about as a result of the submissions made to this committee, whether in written form or in oral form, as we just heard in today's meeting.

This document will include that information, the issues and proposals, organized more or less according to the sequencing of the act. It will also have other background information as necessary, but on that point I would like to note that this issues and proposals document also works in concert with the submission summary document, that the committee received some time ago, because that is a more complete summary of the written submissions that were made to the committee. Also, there are the actual submissions in full form as well that the committee can consult in preparation for the deliberation phase of this committee's review.

I would also make mention of the fact that this issues and proposals document's purpose is to act as kind of a guide for the committee in terms of navigating all the information that the committee has received to this point. However, it is the committee's choice, of course, whether or not to instruct us to prepare this document, first and foremost, and, second of all, whether or not you want to go through all these issues as set out, whether to go through some of them, whether to go through them in the sequence in which

they're laid out, and whether or not to simply deviate from the document and add to those issues and proposals.

There you have it, and I'm able to answer questions if there are any.

The Chair: Do any hon. members have any questions in relation to the issues document? Anyone on the phone?

All right. Seeing none, I would need a member to move a motion for research services to compile this document. Moved by MLA Dach that

> the Standing Committee on Alberta's Economic Future direct research services to prepare an issues document for the committee's review of the Personal Information Protection Act for the next meeting.

All those in favour, say aye. All those opposed? On the phone? Excellent. That motion is carried.

Are there any other issues for discussion before we conclude our meeting?

All right. Seeing none, our next meeting will be held in October. I know that we've all been polled for that date, and we will have that for you shortly.

With that being said, I will call for a motion to adjourn. Moved by MLA Taylor that the September 7, 2016, meeting of the Standing Committee on Alberta's Economic Future be adjourned. All those in favour, say aye. All those opposed? On the phone? That motion is carried, and the meeting stands adjourned.

[The committee adjourned at 2:43 p.m.]

Published under the Authority of the Speaker
of the Legislative Assembly of Alberta