Legislative Assembly of Alberta

The 31st Legislature
First Session

Standing Committee
on
Resource Stewardship

Personal Information Protection Act Review

Tuesday, September 24, 2024
9 a.m.

Transcript No. 31-1-13

Legislative Assembly of Alberta
The 31st Legislature
First Session

Standing Committee on Resource Stewardship

Rowswell, Garth, Vermilion-Lloydminster-Wainwright (UC), Chair
Schmidt, Marlin, Edmonton-Gold Bar (NDP), Deputy Chair

Al-Guneid, Nagwan, Calgary-Glenmore (NDP)
Armstrong-Homeniuk, Jackie, Fort Saskatchewan-Vegreville (UC)
Dyck, Nolan B., Grande Prairie (UC)
Eggen, David, Edmonton-North West (NDP)
Hunter, Grant R., Taber-Warner (UC)
McDougall, Myles, Calgary-Fish Creek (UC)
Sinclair, Scott, Lesser Slave Lake (UC)
Sweet, Heather, Edmonton-Manning (NDP)

Office of the Information and Privacy Commissioner Participants

Diane McLeod	Information and Privacy Commissioner
Cara-Lynn Stelmack	Assistant Commissioner, Case Management
Chris Stinner	Assistant Commissioner, Strategic Initiatives and Information Management

Support Staff

Shannon Dean, KC	Clerk
Trafton Koenig	Law Clerk
Philip Massolin	Clerk Assistant and Executive Director of Parliamentary Services
Nancy Robert	Clerk of *Journals* and Committees
Abdul Bhurgri	Research Officer
Rachel McGraw	Research Officer
Warren Huffman	Committee Clerk
Jody Rempel	Committee Clerk
Aaron Roth	Committee Clerk
Rhonda Sorensen	Manager of Corporate Communications
Christina Steenbergen	Supervisor of Communications Services
Amanda LeBlanc	Managing Editor of *Alberta Hansard*

Transcript produced by *Alberta Hansard*

Standing Committee on Resource Stewardship

Participants

Ministry of Technology and Innovation
Hilary Faulkner, Acting Assistant Deputy Minister, Innovation, Privacy and Policy
Meredith Giel, Director, Access Policy and Privacy

The Nonprofit Chamber
Karen Ball, President and CEO
Alexa Briggs, Vice-president, Policy and Research

Office of the Information and Privacy Commissioner for British Columbia
Michael Harvey, Information and Privacy Commissioner

Office of the Privacy Commissioner of Canada
Philippe Dufresne, Privacy Commissioner

9 a.m. Tuesday, September 24, 2024

[Mr. Rowswell in the chair]

The Chair: Okay. I'd like to call this meeting of the Standing Committee on Resource Stewardship to order and welcome everyone in attendance.

My name is Garth Rowswell, MLA for Vermilion-Lloydminster-Wainwright and chair of the committee. I'd ask that members and those joining the committee at the table introduce themselves for the record. We'll begin to my right. Go ahead.

Ms Armstrong-Homeniuk: MLA Jackie Armstrong-Homeniuk, Fort Saskatchewan-Vegreville.

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

Mr. Dyck: MLA Nolan Dyck, Grande Prairie.

Ms Faulkner: Hilary Faulkner, acting assistant deputy minister of innovation, privacy, and policy with Alberta Technology and Innovation.

Ms Giel: Meredith Giel, director of access policy and privacy, Technology and Innovation.

Mr. Eggen: Good morning. My name is David Eggen. I'm the MLA for Edmonton-North West.

Mr. Schmidt: Marlin Schmidt, Edmonton-Gold Bar.

Ms Sweet: Morning. Heather Sweet, MLA, Edmonton-Manning.

Mr. Bhurgri: Good morning. Abdul Aziz Bhurgri, research officer.

Ms Robert: Good morning, everyone. Nancy Robert, clerk of *Journals* and committees.

Mr. Huffman: Good morning. Warren Huffman, committee clerk.

The Chair: Okay. We'll now go to those joining us online. Please introduce yourselves as I call your names. MLA Al-Guneid, go ahead.

Ms Al-Guneid: Good morning, everyone. Nagwan Al-Guneid, the MLA for Calgary-Glenmore.

The Chair: MLA McDougall.

Mr. McDougall: Hello. Myles McDougall, MLA for Calgary-Fish Creek.

The Chair: MLA Sinclair.

Mr. Sinclair: Good morning, everybody. Scott Sinclair. I'm the MLA for Lesser Slave Lake.

The Chair: Okay. Thank you.

There are no substitutions today.

A few housekeeping items to address before we turn to the business at hand. Please note that the microphones are operated by *Hansard* staff. Committee proceedings are live streamed on the Internet and broadcast on Alberta Assembly TV. The audio- and videostream and transcripts of the meeting can be accessed via the Legislative Assembly website. Those participating by videoconference are encouraged to please turn on your camera while speaking and mute your microphone when not speaking. Members participating virtually who wish to be placed on the speakers list are asked to e-mail or message the committee clerk, and members in the room are asked to please signal the chair. Please set your cellphones and other devices to silent for the duration of the meeting.

For approval of the agenda are there any changes or additions to the draft agenda? If not, would someone please make a motion to approve the agenda? MLA Schmidt. Any discussion on that? Okay. All in favour? Any opposed? Online, all in favour? Any opposed? Thank you. That is carried.

Next the minutes. Next we have the draft minutes for the June 28, 2024, meeting. Are there any errors or omissions to note? If not, would a member like to make a motion to approve the minutes? MLA Hunter. Any discussion? All in favour, say aye. Any opposed, say no. Online, all in favour, say aye. Any opposed, say no. Okay. That is carried.

Review of the Personal Information Protection Act. We now have our oral presentations. Hon. members, at our June 28, 2024, meeting the committee agreed to hear oral presentations related to our review of the Personal Information Protection Act. As members will recall, the committee invited the Information and Privacy Commissioner of Alberta to make a presentation. In addition, the government caucus and Official Opposition caucus each had an opportunity to select up to three other individuals or organizations to invite and make presentations to the committee. The six groups invited to present were the Ministry of Technology and Innovation, the office of the Information and Privacy Commissioner for British Columbia, the office of the Privacy Commissioner for Canada, the Calgary chamber of voluntary organizations, the Law Society of Alberta, and the Faculty Association of the University of Calgary. Unfortunately, the faculty association and the Law Society are not able to present.

As laid out in the agenda, we will hear a presentation from the ministry first, followed by the Calgary chamber of voluntary organizations. Both will have 15 minutes to present, with time for members to ask questions after each presentation. After that, the three commissioners will present as a panel. Each commissioner will have up to 15 minutes to make their presentations, and then there will be a joint question-and-answer period for members to ask questions of any of the commissioners.

The Ministry of Technology and Innovation is first up. We would like to invite Hilary Faulkner and Meredith Giel – okay? – with the Ministry of Technology and Innovation. You have 15 minutes to make your presentation. Please introduce yourselves for the record prior to beginning your presentations. You may start.

Ministry of Technology and Innovation

Ms Faulkner: Good morning, Chair, members of the committee, and others present. My name is Hilary Faulkner. I am the acting assistant deputy minister of innovation, privacy, and policy with Alberta Technology and Innovation. With me today is Meredith Giel, who's the acting executive director for privacy, policy, and governance. We appreciate the opportunity to be back here today to talk with you further about the Personal Information Protection Act, or PIPA, and specifically about amendments that could be considered as part of the review.

Moving on to slide 2, before I speak to specific areas for consideration, I want to first take a moment to reinforce the importance of PIPA. Albertans are concerned about privacy and expect organizations to have robust privacy protections in place. They expect them to be accountable for breaches or misuse of personal information and to be transparent around data handling practices. PIPA provides individuals with a number of rights, including the right to ask an organization to see the personal

information it has about them, to find out how that information is being used or disclosed, and to ask for corrections if they believe a mistake has been made.

As risks to personal information like identity theft and privacy breaches increase as the world becomes more digital, sound privacy practices benefit all organizations and the people they serve in a number of ways. These include protecting against harm and other negative outcomes, producing better quality data that leads to better outcomes, and improving transparency and, by extension, trust. Effective privacy legislation must address several key considerations to balance the privacy of individuals while also allowing organizations to operate innovatively, effectively, and responsibly.

Moving on to slide 3, for the purpose of today's presentation I want to quickly highlight some of the key areas for the committee's consideration, which we spoke to in our formal submission to the committee earlier this year. These include the changing legislative landscape and an opportunity to harmonize our legislation with other jurisdictions, the scope of the act and whether this needs to be broadened, the inclusion of individual data rights, the enhancement and strengthening of privacy protections, the introduction of new categories of data and rules around them, and reviewing and strengthening offences and penalties.

Moving on to slide 4, since PIPA was enacted in 2004, the legislative landscape in Canada and around the world has significantly changed. Harmonizing privacy legislation is important as it would empower businesses and organizations in Alberta to operate efficiently across different regions while ensuring that consistent privacy practices and protections are maintained regardless of geographic boundaries. It would help create a more secure environment for data protection, benefiting both individuals and organizations.

As part of its recent review British Columbia's Special Committee to Review the Personal Information Protection Act stressed the importance of harmonization with the changing legislative landscape, with a focus on new provisions for the rapidly changing digital world. When looking at other jurisdictions, consideration could be given to aligning with certain principles within the European Union's General Data Protection Regulation, or GDPR, and Quebec's Law 25. The GDPR is considered to be the most robust privacy law for its comprehensive scope, strong data protection principles, enhanced individual rights, strong penalties and enforcement, and data security. Quebec, which is currently touted as the strongest privacy law in Canada, recently amended its Act Respecting the Protection of Personal Information in the Private Sector with key amendments focusing on privacy breach notification, privacy protection mechanisms, and individual rights.

9:10

In addition to looking outside of Alberta, the current review of PIPA presents an opportunity to increase alignment with other pieces of privacy legislation in the province. Amendments could consider establishing common definitions and enhancing interoperability between the three different sectors covered by these laws. By aligning provisions where possible, Alberta could streamline compliance efforts and promote consistency and privacy practices across the private, public, and health sectors. Alberta will also need to pay close attention to federal Bill C-27 as, if passed, it may impact Alberta's substantially similar status and require potential amendments.

Moving on to slide 5, we have also heard that there is a need to review the scope of PIPA, particularly as it relates to nonprofit organizations and political parties. Currently PIPA only applies to nonprofit organizations when they collect, use, or disclose personal information in connection with a commercial activity. No other legislation applies unless a nonprofit organization is acting under contract with a government or a company.

The inclusion of nonprofit organizations could be done in a couple of different ways. The first would be to define commercial activity to resolve the lack of clarity and help nonprofits better understand their obligations under the act, reducing the risk of noncompliance due to ambiguity within the scope of commercial activity. Alternatively, the committee could also consider extending the scope of PIPA to include nonprofit organizations. The committee could also consider extending PIPA's scope to include political parties. This would align with privacy laws in both British Columbia and Quebec. Expanding the scope of PIPA to fully encompass nonprofit organizations and political parties would enhance transparency, accountability, and privacy protection within these sectors. However, it will also be important to examine the additional compliance burdens and operational challenges that this may create and ensure that there is a pathway to reduce this as much as possible.

Moving on to slide 6, while PIPA establishes rights for individuals regarding the collection, use, and disclosure of their personal information, it lacks provisions for several key rights which are recognized in other jurisdictions. These include the right to erasure, or the right to be forgotten; the right to data portability; and the right to object to specific data processing activities such as automated decision-making or artificial intelligence systems. These rights are central to modern legislation as they ensure that individuals have and maintain control over their personal information. They promote transparency, prevent misuse, and provide avenues for addressing violations. Individual data rights play a key role in establishing a balanced approach to data protection that respects the privacy of individuals and the needs of private-sector organizations.

Moving on to slide 7, protecting personal information from unauthorized access user disclosure is critical to preserving individuals' privacy rights. As greater amounts of information are managed by private-sector organizations, public concerns around the collection and use of personal information have correspondingly increased, particularly because of information being exploited or mishandled. Introducing new mandatory requirements for organizations to develop and implement privacy management programs and privacy impact assessments would enhance privacy protections and increase accountability for private-sector organizations that are entrusted with Alberta's personal data.

Currently PIPA requires organizations to notify the office of the Information and Privacy Commissioner if a privacy breach occurs that poses a real risk of significant harm. Reviewing breach reporting requirements to determine whether current provisions remain appropriate will enhance transparency and accountability for organizations handling personal information.

Moving on to slide 8, a key tool for protecting privacy involves creating new categories of data in which personal information is removed or anonymized. This allows organizations to work with raw data while mitigating the risk of individuals being identified. These types of data can be powerful tools for research as they allow organizations to identify trends, analyze interdependencies, and develop targeted initiatives without exposing individuals' personal information. By authorizing the creation of this type of data and putting in place specific transparency provisions if personal information is used in this way, this would balance the potential to harness this information for research and innovation while also ensuring that Albertans are aware of how their data is used and processed.

In addition to these new categories of data, another type of data which the committee could consider is sensitive data. With the rapid evolution of technology, there is a growing concern around

safeguarding sensitive data and protecting children's privacy. Sensitive data includes things like medical, biometric, or intimate personal information, and it can also include children's data. These types of information have a higher expectation of privacy due to the potential to result in serious harm if compromised. As technological advancements continue to expand the scope of personal data collection and processing, it is critical to strengthen protections for such information under PIPA.

Moving on to slide 9. The last consideration I want to highlight for the committee today is around offences and penalties. Enforcement measures are essential to ensure compliance with privacy regulations and to deter noncompliance. Currently PIPA contains penalties for noncompliance within its regulations, but there are no provisions which allow for administrative monetary penalties, or AMPs. AMPs are financial penalties imposed by regulatory agencies rather than through the criminal justice system. The lack of this sort of penalty limits the options available to the office of the Information and Privacy Commissioner in enforcing the legislation. Other jurisdictions have introduced AMP provisions in their laws to address serious, repetitive, or long-term contraventions and to reinforce that individuals' privacy rights are protected and enforced. For example, Quebec's legislation allows for its regulator to impose AMPs and it sets out terms for recovering and claiming the amounts owed.

According to the GDPR AMPs should be effective, proportionate, and dissuasive. While AMPs are intended to deter noncompliance, it is important to recognize that a flexible and risk-based approach must be considered to accommodate the various operational needs and resources of organizations in Alberta. While penalty amounts should be set at an appropriate level to deter noncompliance, care must be taken to ensure that AMPs do not have an outsized impact on small businesses or stifle innovation and competitiveness in the province.

Moving on to slide 10. Protecting privacy is a priority for the government of Alberta. The key considerations that I have presented here today have the potential to significantly improve life for Albertans and are critical to protecting Albertans' privacy, enhancing the trust of Albertans, and ensuring private-sector organizations are effectively able to meet privacy challenges now and into the future.

Thank you for providing me with the opportunity to present today.

The Chair: Okay. Thank you very much for your presentation.

Now we'll open the floor to questions, and we'll go back and forth and have the main question and then a follow-up. MLA Dyck, go ahead.

Mr. Dyck: Well, excellent. Thank you so much, Chair. Thank you for coming and presenting. This is actually kind of exciting to me, so thank you for doing this. Yeah. Just a question around some of the portability. I know that the EU has their general data protection regulations, which include, really, I guess, the big three: right to erasure, the right of data portability, and the right to object to specific data processing activities. I don't believe we currently have this in Alberta, so we're a little behind here, but can you explain just the implementation of what this would look like specifically for our large audience watching this committee right now and just how the individual data rights increase the security, and then can you also give a specific example on how data portability might be used and a specific example on the right to object to specific data processing activities, how the outcome of that might happen?

Ms Faulkner: Thank you. Just to ensure I heard the question accurately: specifically speaking to implementation of the three components mentioned from the GDPR related to erasure, the right to object, and data portability, and examples related to data portability and – sorry; I missed the other one.

Mr. Dyck: Oh. The data portability and the right to object to specific data processing activities. I just need some examples, firm examples of how that would be implemented or how companies would be able to execute this.

Ms Faulkner: I think, first, in terms of implementation from the department's perspective, we would definitely want to work with industry and businesses on exactly what those measures could look like. It is helpful that the GDPR has already implemented these measures, and with the already, I'd say, highly connective world that we live in, a lot of businesses are already very aware, particularly large businesses, but for smaller organizations and businesses and even medium-size businesses I think that's going to be a really important, I guess, consideration for the government of Alberta in terms of ensuring that we are taking into account all of their issues and concerns and how those can be mitigated.

9:20

In terms of the right to object, my understanding right now of how that works within the GDPR and recognizing that the European Union is comprised of multiple different states, there is the opportunity within the legislation for them to object specifically to the organization about, I guess, the first case, they would have to be aware of how the information is being used or there are transparency provisions that require that information to be provided in a plain, concise language so that people can understand, and then understanding that they have a right to object, I believe it's through either the regulator or through the organization itself, to identify that they do not want their information to be used for that purpose. Implementation within Alberta could look very similar. We do have a regulator with the Information and Privacy Commissioner. That would obviously be additional scope for them, and provisions would have to be allowed for that within legislation.

In terms of data portability, I think that similar, I guess, considerations would have to be made particularly on the engagement side to understand how organizations are being used. I'd maybe ask, Meredith, if you have any specific examples of how that would be used.

Ms Giel: Yeah. In terms of how data portability would work, essentially, if an individual has been working with a private organization, and they decide that they do not want to use that organization and instead want to move to a different organization, they can request that organization essentially port their personal information over to the new organization that they are willing to work with, essentially ensuring the transfer of their personal information from one organization to another.

Mr. Dyck: Excellent. Good. Thank you.

The Chair: Did you have a follow-up?

Mr. Dyck: I think just on the data portability. So this is more their personal information on an individual side, not on an employee side of data collected. That is correct?

Ms Giel: Correct.

Mr. Dyck: Excellent. Thank you.

The Chair: Thank you.

Our next question is from MLA Al-Guneid. Go ahead.

Ms Al-Guneid: Hi, everyone, and, yeah, thank you for your service and for being here. My question is on the right to be forgotten and the right to be informed about automated decision-making and AI systems. I'm actually glad to see these two specifically in your slides, because it's very timely. There are recent developments we're seeing in the last few weeks, so I hope the department is following it very closely.

First, we heard about what LinkedIn is doing. If you are a LinkedIn user outside the EU, which means you are not under the GDPR, you've just been sneakily opted in, which means it lets LinkedIn and its associates to clone your post without crediting you. Basically, LinkedIn can use your intellectual property to train their automated content creation using generative AI systems. And just quickly to be clear for everyone's sake, what we mean by generative AI: it's creating new content, text, images based on the patterns we're seeing in data. That's what we call the large language models, or LLMs, so that's ChatGPT, Gemini, and Claude AI. I do recognize that the regulation of AI is beyond the scope of PIPA, but there are significant privacy concerns here related to PIPA.

I just want to be clear here as well. The problem is not that LinkedIn is training AI systems on our data. No, that's business as usual, actually, on the Internet. The problem here is about data deletion, which takes me back to your slides on the right to be forgotten and the right to be informed of automated decision-making and AI systems. We, as consumers of LinkedIn, Facebook, and all these apps, have the right to delete our data if we ask these social networks to delete them, but we cannot achieve data deletion with the new system. It's actually baked in. It's like sugar in a cake. You can't take it out anymore.

So two questions for you. Are you following the generative AI developments closely and how it impacts Albertans' rights to be forgotten, and if yes, what are the ministry's next steps? And then the second question is: how is the government collaborating with the federal government on this issue specifically? It's not just a provincial issue, and probably the ministry will be limited in finding solutions.

Thank you.

Ms Faulkner: Thank you very much. In terms of your first question, yes, we are following very closely the developments in relation to artificial intelligence, both in terms of what we're seeing on the technology side but also on the policy and regulatory side. In terms of that, I'd say we are seeing a lot of different jurisdictions approaching things in different ways. Privacy legislation is definitely one of the ways that jurisdictions are addressing artificial intelligence, particularly now as it relates to personal information and the protection of privacy. We're watching that very closely. Very interested in this committee's review and any recommendations related to the Personal Information Protection Act and how that may or may not relate to the use of artificial intelligence, particularly for Albertans.

And then in terms of next steps for the ministry, I would say that we're taking a very, say, pragmatic and principled approach to looking at what options Alberta has for jurisdiction, for regulating, I guess, and legislating in this area. We are watching Bill C-27 very closely. As you know, not only does it address privacy, but it also has the Artificial Intelligence and Data Act in there as well. So we're working closely with the federal government on that not only in terms of what impacts it has on the province but what that will mean for Albertans. And then, I guess, exploring what other gaps or challenges there might be and how Alberta can address that.

The Chair: Did you have a follow-up question to that?

Ms Al-Guneid: It's just an evolving situation, so I'm curious. This happened, like, last week – sorry; two weeks ago – the LinkedIn situation, and last week the United Nations released a whole AI framework because they're finding it problematic. The whole AI regulation is problematic at a local and provincial and national level. So this is not an Alberta issue; this is a national issue; it's a global issue. So I would just love, I mean, as things progress, to get more details on: how are we actually collaborating with others on this? Like, it is an evolving situation.

The Chair: Did you – you're good?

Ms Faulkner: Yes, I'm good.

The Chair: Okay. Great.

Our next question comes from MLA Hunter. Go ahead.

Mr. Hunter: Thank you, Mr. Chair, and thank you for being here this morning. When I was the red tape reduction minister, I had a lot of small businesses approach me and talk to me about, you know, the difficulty of being able to have that compliance and having to be able to hire compliance officers, yet I know that it's important that we have, as Ms Al-Guneid just stated, a balance, a proper balance. I also was contacted by many health professionals that say that there are ways of being able to use data to innovate in the health space. So how does the ministry find the balance, and how does PIPA create that balance between, you know, what's good for helping small businesses, which are disproportionately affected by that because they just don't have the money for compliance officers, and being able to make sure that we have proper PIPA rules?

Ms Faulkner: Great question. Thank you. Yeah. That's definitely something that's really important for Alberta in terms of both legislation but also the impacts to businesses. In terms of finding that balance, it's really important to look at any new provisions or requirements in terms of the size and scale of an organization as well as looking at it from the type of information that they're collecting and using. Those can be both in terms of how you look at a privacy management program, what privacy impact assessments are required, privacy breach reporting protocols: those types of things can all be tailored depending on the type of information, the size and scale of the organization, and that type of thing.

I also think there are opportunities. From the government side of things we put out a lot of information to support businesses in terms of understanding what privacy protections are required, their obligations under the legislation. We have different guides, and we have a helpdesk and other supports that we can offer to support them through that, given that it is critical that Alberta's privacy protections are strong and protected but also, at the same time, that it's not overly burdensome on an organization.

9:30

Mr. Hunter: Just a follow-up, Mr. Chair. How does scale affect – I mean, it's the same law. It's the same application. How can you address the scale issue?

Ms Faulkner: I'd say the requirements for an organization, maybe a – I don't know what an excellent example here would be. Maybe, like, a large energy company versus a company that's – I don't know – a clothing store owner in a small town. Both are collecting

potentially personal information, but what that looks like in terms of assessing the risk with that information for a clothing store owner – perhaps that's more related to their client information, how they're protecting that in terms of their security systems that they have in place, how they are obtaining consent from their customers, that type of thing – will look much different. So from a scale perspective, I think it's just understanding the amount of resourcing that an organization has and can put behind it between a large or small organization.

I'd also say to the other aspect, to your earlier point about health information, we do have the Health Information Act that plays in there, too, but health information is very critical information for people. It's important that it's protected, so health information and how that is used by an organization may be handled or should be handled differently than perhaps other information.

The Chair: MLA Eggen, go ahead.

Mr. Eggen: Yes. Thank you, and good morning. You mentioned that there is impending legislation, C-27, federally, and you also said that you're watching that closely. Have you itemized some provincial legislation that we might have to modify if and when C-27 gets passed federally?

Ms Faulkner: PIPA is probably the, I guess, biggest piece of provincial legislation that we're watching specifically. Right now PIPA is considered substantially similar to the federal privacy legislation, which means that companies in Alberta who follow this legislation are equivalent to federal legislation. Not all provinces have private-sector privacy legislation. Alberta is a little bit different than other provinces in that regard, so it is important for our businesses in terms of competitiveness and efficiency that we don't have multiple pieces of legislation that would apply to them. That creates confusion, a lack of clarity, that type of thing. So I'd say PIPA is the biggest piece of legislation that we're watching in regard to Bill C-27.

Other aspects of that bill, which I spoke a little bit to earlier, do relate to artificial intelligence and data, so we're watching those as well in terms of what impacts across kind of multiple pieces of legislation there could be.

Mr. Eggen: Thank you.

Perhaps you could offer some more specific information as to what needs to be harmonized and/or amended here provincially as this Bill C-27 moves forward. As the MLA for Calgary-Glenmore mentioned, and you did, too, it's really important for us to harmonize our privacy legislation both nationally and internationally. If you could just give us a running – you don't have to do it here orally, but just give us a sense of what specifically needs to be amended provincially so that we are in harmony with federal law.

Ms Faulkner: I would say I don't – at this time I can't provide necessarily a specific list. Happy to follow up on that. I think for us, we're still watching. It's still under discussion, so still paying attention to everything to ensure that, I guess, with the final bill, at the end of the day, we understand that and we understand the legislation, and then we can do, I'd say, a more comprehensive review to understand any amendments we have to make.

Mr. Eggen: Okay. Great. So that's, like, a follow-up in writing. Thanks.

The Chair: Next question comes from MLA Dyck. Go ahead.

Mr. Dyck: Excellent. Well, thank you so very much, Chair, again. Just in Technology and Innovation here, the report you guys submitted, just on – and I believe it was slide 5 or 6 – nonidentifying data, anonymized data, and synthetic data: there's a huge opportunity for research to be here as well as for that service deliverability for Albertans. Can you expand a little bit more on the service deliverability, of what that looks like in a framework, for me? There were a couple of examples, but I just want more of a framework idea. How do we actually – that, to me, is the opportunity that companies are going to be looking at, or individuals potentially, as they research how we can actually protect data and also serve the people of Alberta in clear and concise ways. Can you just expand on that, to bring a little bit more on the service deliverability side of things?

Ms Faulkner: Sure. In terms of, I guess, nonpersonal data, so data that has been taken and then anonymized or nonidentified, the data world, I would say, has much different terms for how each of those different types of data is identified and used, but at the end of the day it means that that information can be used in a way that protects privacy and protects people's personal information.

In terms of service delivery I think for organizations, as it was mentioned earlier, you know, a lot of them are already doing this, where they're taking information and training it for generative AI or they're deidentifying it already without there necessarily being provisions in place. They're doing this, and then that information is offering them insights into how they can improve, I guess, their products, how they can improve their services, their marketing, different aspects like that.

I don't know, Meredith, if you have a specific example that we've come across.

Ms Giel: Not a specific example, but I think in terms of the regulatory framework around it we would need to make sure that the legislation is looking at the techniques that are being used in order to anonymize or modify that data to make sure that it is not able to identify an individual or reidentify an individual. Also, making sure that there are appropriate security arrangements in place for that information, thinking about the circumstances under which that information can be shared, really making sure that although the data should be created in a way that can't be identified, with the way that technology is evolving, there is that risk that remains in terms of reidentification, so making sure that there are the appropriate controls in place to make sure that even though organizations are sharing and using that information, Albertans can be confident that their privacy is protected and there won't be unnecessary breaches associated with that because proper techniques haven't been used.

Ms Faulkner: I would add to that, too, that with having the Information and Privacy Commissioner as our regulator, that's a key role as part of the framework. And while we don't necessarily have those provisions now in the legislation, should they be added, there would need to be corresponding provisions added in relation to the role of the regulator.

Mr. Dyck: A follow-up if I may?

The Chair: Yeah. Go ahead.

Mr. Dyck: So for an individual in our framework, for an organization that has the data, that is looking to look through their data to find these outcomes to make their product better – they have all the information, the personalized information – are they going to need to anonymize or deidentify the data before utilizing that since they already own that individual's data? Would that be the

suggestion from you, or is this only on the research side? Like, I'm asking: on the internal research of a company that maybe has large-scale data, are you also suggesting that they have to deidentify internally in order to make sure that their staff or team cannot identify within their data as well?

Ms Faulkner: I would say it depends on what they're using it for and who they're sharing the information with within their organization. So it would be very dependent on the use case and what they intend to do with that. For an organization that already has the data and has been given consent to use it for whatever purposes they had identified when they were collecting that information, they don't necessarily have to deidentify it if they already have that consent. This just gives organizations that opportunity, and it clarifies for Albertans that this could be a way that their data and information is used.

Mr. Dyck: Okay. Thank you very much.

The Chair: Any others? Okay.

I would like to thank Ms Faulkner and Ms Giel for your presentations and for joining us here today. You are welcome to return to the gallery and watch the remaining presentations or depart if you wish to do so. Thank you very much.

Next we will be joined online by Karen Ball and Alexa Briggs with the Calgary chamber of voluntary organizations. You will have 15 minutes for your presentation. Are you ready to go? You're set up to go? Okay. Good. Please introduce yourselves, and begin when you are ready.

9:40

Thank you very much.

The Nonprofit Chamber

Ms Briggs: Good morning, everybody, from Calgary, Mohkinstsis. My name is Alexa Briggs. I'm the vice-president of policy and research with what is now known as the Nonprofit Chamber. We just changed our name from CCVO. With me here is our president and CEO, Karen Ball. I'll do a short presentation, and then we're very happy to answer any questions. Thank you very much to the committee for the invitation to make this presentation on behalf of the nonprofit sector's needs. We're very grateful for the opportunity.

Just a little bit about us. The Nonprofit Chamber is a member-based charitable organization established in 2004 to strengthen the vibrant nonprofit sector and address sector-related public policy issues in Alberta.

Just a little bit about the nonprofit sector in Alberta. Our sector fills critical needs for the province: food and basic needs, immigrant settlement supports, senior and child care supports, sports and recreation, arts and culture, entrepreneurship, environmental health, and more. We provide the social capital, services, and infrastructure critical to attracting workers across all sectors. The full spectrum of services and activities provided by our essential sector make Alberta a great place to live, work, and play in a rapidly changing, competitive global economy.

Our sector employs 285,000 people in Alberta, 78 per cent of whom are women, and contributes 5 and a half billion dollars to our GDP while leveraging an astounding 227 million volunteer hours annually. If the volunteer labour were conservatively valued at $21 an hour, it amounts to nearly another $5 billion.

Approximately half of Alberta's nonprofits operate with no staff. They are run fully by volunteers. All nonprofits are governed by a volunteer board of directors, so even those nonprofits with staff capacity are operating with the contribution of significant volunteer time. Most Alberta nonprofits are small organizations. For example, 87 per cent of Alberta charities have annual operating budgets under a million dollars, and 52 per cent of charities have budgets under $100,000.

Now just on to PIPA and what it means for our sector. As noted on the government of Alberta's website on PIPA, PIPA is Alberta's private-sector privacy law. As such, it only applies to nonprofits for information collected, used, or disclosed for commercial activity such as selling membership lists. This principle was established when the legislation came into effect in 2004 and was upheld in the 2015 comprehensive review of the legislation.

The government of Alberta has created an excellent site dedicated to PIPA and nonprofits. This site provides nonprofits with three critical supports: first, a clear explanation of what is included in commercial activity, most pertinently for many nonprofits that accepting donations for charitable purposes is not a commercial activity; second, valuable resources to help nonprofits determine whether or not they're subject to PIPA and how to comply with the legislation; and, third, sample statements, forms, and policies. I would just like to take a moment to say thank you for all of that outstanding work to date, that has been hugely supportive for the sector.

The current approach to PIPA and Alberta's nonprofits is effective and efficient. We have had no request to change this legislation as it relates to nonprofits, nor are we aware of any issues that have arisen as a result of the current approach. In fact, we note with interest that since the legislation was in effect in 2004 – that's 20 years – just 60 complaints related to nonprofits have been logged. Just for some very easy math, that would work out to three per year.

Moving on to the potential impact of changing to a blanket approach to PIPA for the nonprofit sector, given limited resources and access to legal expertise, the majority of Alberta nonprofits will not have the capacity to readily interpret and comply with any changes to this legislation that broaden its scope to apply to all nonprofit activities beyond the commercial activities to which it already applies. Additionally, many nonprofits are already in compliance with other pieces of privacy legislation such as the Health Information Act or FOIP. Broadening the current approach for nonprofits within the PIPA legislation will cause confusion among the sector, add workload to an already stressed sector, and create red tape for the government of Alberta and nonprofits alike. It would require resources, education, and training for nonprofits to comprehend and comply while not increasing the privacy protection of Albertans from commercial interests.

But for the purposes of this review we have one request and one offer: we respectfully request maintenance of the current approach with this legislation and its application to nonprofits in Alberta for commercial activity, and we offer to promote the existing government of Alberta PIPA resources for nonprofits, which include best practices for handling personal information. The Nonprofit Chamber and our partners would be pleased to support the government of Alberta in promoting the existing PIPA resources through our extensive reach with Alberta's nonprofits. I would say, also, any upgrades or changes that are made: we'd be super happy to promote that.

In sum, the purpose of this legislation is to protect personal information from commercial use, and it is fulfilling that purpose now for a nonprofit. There's no purpose to extending the regulation. Nonprofits should be enabled to provide their vital contributions to our communities while offering reasonable protections that do not take away from their ability to focus on their organizational mission. Introducing a blanket application of PIPA to nonprofits

will create unnecessary red tape, confusion, and administrative workload for both the nonprofit sector and for the GOA. Please carefully consider the stakes for the nonprofit sector in your review against what will likely be adverse outcomes for the sector and uncertain or unlikely positive outcomes in changing PIPA as it stands with regard to the nonprofit sector.

Thanks for your time. Happy to take any questions.

The Chair: Okay. We will now open the floor up to questions. MLA Armstrong-Homeniuk, go ahead.

Ms Armstrong-Homeniuk: Thank you. Chair, through you and to the Calgary chamber, I'd like to ask a few questions. Good morning, ladies. I acknowledge and thank you for your service and all the good work that you do. I know that in the last couple of years you've been very busy, particularly with the file I'm on with the Ukrainian evacuees, so thank you for all the good work that you do.

In order to keep up with the ever-evolving landscape of technology and information privacy obligations, changes must be made to keep PIPA up to date and in line with national and international privacy legislation changes. In your submission you shared that you consider that PIPA is currently effective and efficient when it comes to the operation of nonprofits; however, we received some submissions asking for PIPA to apply fully to all nonprofit organizations rather than only for commercial activities. In your submission you expressed concerns about further changes to Alberta's PIPA legislation as nonprofits may not have the capacity to keep up with legislative changes within PIPA due to their limited resources and access to legal expertise. Could you elaborate on some of the concerns that your organizations may have in regard to any potential changes to PIPA to include all activities and what these changes would mean in practice for voluntary organizations?

Ms Briggs: Thank you so much for the question. Yeah. I think, you know, as mentioned in my remarks, most Alberta nonprofits are operating with significant voluntary capacity, so the capacity for those volunteers to be able to have the time, energy, and expertise to review and interpret those changes would be significantly taxing, and we have in recent years seen a decline in volunteerism, so this would be one additional stressor for that sector and potentially a deterrent for volunteers, which are crucial. They are crucial for most nonprofits.

Karen, do you have – I'll just let Karen jump in if she's got anything to add to that.

Ms Ball: Thank you, and thank you for your great work on the Ukrainian file. We enjoy being part of it. We appreciate it.

Thanks for the question. I would just also add that there are 30,000 nonprofit organizations. They are obligated to comply with PIPA for commercial purposes, which as I understand is the purpose of the regulation. It would be the responsibility of the government of Alberta to bring them to compliance if it was broadly applied, so this is also a large piece of red tape on both sides, both for nonprofits and also for the government of Alberta to ensure compliance of a nature with this many organizations and, as Alexa said, mostly operating with volunteers who, as you know, change from year to year, so you are dealing with different people on a constant and ongoing basis. So it would not be a one-time responsibility of the government but ongoing.

Thank you.

9:50

Ms Armstrong-Homeniuk: It is my understanding that in the past, around 2007, when not-for-profit organizations were included for commercial activities to the PIPA legislation, there was a one-year transition period. Would something like this be able to alleviate some of the concerns you have?

Ms Briggs: I don't think giving more time is really a good solution here simply because of what Karen just mentioned. You know, volunteers change from year to year, so there will be constant renewal within the nonprofit sector. It isn't just about the time; it's also the capacity to be able to implement, interpret, and then apply any of the changes.

Ms Ball: Maybe I'll just add to that that the organizations that do have commercial purposes and use information in that way tend to be the larger organizations, so perhaps a transitionary period for those organizations saw some results that you're not going to see in a blanket approach.

Thank you.

The Chair: Thank you.

From the opposition, is there – NDP caucus, no questions?

Okay. Go ahead. You've got another one.

Ms Armstrong-Homeniuk: Thank you. Chair, through you to the group here again: I was glad to see in your submission that the government of Alberta currently has some resources and a web page dedicated to explaining how PIPA currently applies to the nonprofit sector for commercial activities. Alberta's government will always support the incredible work of our nonprofit sector and want to ensure you are successfully able to understand and ultimately comply with PIPA and any legislation that involves nonprofits. Are there any supports that you think the government could provide to ensure successful engagement for nonprofit organizations and a good understanding for any potential changes of PIPA legislation?

Ms Briggs: Yes. We're happy, as I said, to continue to support efforts to share the existing resources or any additional resources that are created and also making good use of the portal that's been created by the Ministry of Arts, Culture and Status of Women. They have also a really great bank of resources that are dedicated to the nonprofit sector, and adding those there would be wonderful.

I would say that if there are significant changes that are made, resources and the transition period would simply not be sufficient. It would have to come with financial support and significant education and training efforts that are done with considerable vigour and expertise.

Ms Armstrong-Homeniuk: Thank you.

That's all for me.

The Chair: Go ahead, MLA Hunter.

Mr. Hunter: As I get older, my memory is not so good, but just if you could remind me: this was also presented back between 2015 and 2019, to have these changes, wasn't it? Can you remind me about what happened there?

Ms Briggs: I wasn't with the organization at that time. I've looked at some of what the previous submissions were in the previous review of PIPA legislation. I'm interpreting the question correctly?

Mr. Hunter: Yeah.

Ms Briggs: Yeah. I believe that recommendation was made, and the approach that currently stands to apply PIPA to nonprofits that engage in commercial purposes with the personal information was upheld, and the approach was kept as it was.

Mr. Hunter: Yes. So at the time it was felt that there was just too much on our volunteers to be able to move forward. Is that correct?

Ms Briggs: I believe it was in large part the administrative burden that was at the root of it and also sort of the notion, you know, like: for what purpose would the regulation or the legislation be changed?

Mr. Hunter: Yeah. Okay. Good. I just wanted to make sure I remembered that correctly. Thank you.

The Chair: Thank you.

I have a question from MLA Al-Guneid. Go ahead.

Ms Al-Guneid: Thank you, Chair, and thank you, both, for being here and for all the good work that the Nonprofit Chamber does. Congrats on the rebrand.

You've mentioned that you wouldn't want to see an expansion of PIPA in the not-for-profit sector, and you did mention the monetary challenges and the budgetary challenges for the many members you have. If the expansion goes forward, can you tell us more about the impact? What would your organization do to help, and what would your role be? I'm just curious, like, if you can specify some consequences to the sector for the committee's knowledge and understanding.

Thank you.

Ms Briggs: I saw Karen on mute. Go ahead.

Ms Ball: Maybe I'll jump in. Thank you very much. We appreciate your kind words about the sector and the work that you do to support us.

Thanks for the question. A couple of things on that. I would say that, ultimately, the training and ensurance of the compliance of a change of this nature remains the responsibility of the government of Alberta. We would certainly work to help direct nonprofits to supports that are available on the government of Alberta side, but as all things with 30,000 organizations, over half of them being volunteer led, it's often difficult to communicate broadly on changes of this nature to a sector, so I think we would have some basic issues with just ensuring that people understood that the change was happening, what the change meant, and being able to communicate that to them. In the case of a largely volunteer-led sector, there are always a lot of questions when regulatory changes of this nature take place, so I think that there would be probably a massive impact around the effort required to communicate to those organizations on the government side.

From the nonprofit side generally I would say that there are a couple of things. One is that we know that our nonprofit sector has a deficit in terms of digital tools available to them, so the ability to track and monitor using tools and technology that make this kind of process easy actually might be more challenging for nonprofits, who often don't have up-to-date technology in place to be able to do this kind of work. Without the tools in place the kind of process that would be possible for them might be quite onerous.

Then, what we have seen is that, obviously, there's demand on our essential nonprofit services, and when items of this nature become part of that demand, nonprofits have to make a choice. They can't raise their prices; they can't hire more people to respond to this kind of thing. What ends up happening is that they end up having to triage some of the programs and services that they provide, so it actually does have a downstream effect on the essential services – seniors care, youth engagement, these kinds of things that happen in the community – when resources have to be put against things of this nature.

The Chair: Okay. Did you have a follow-up?

Ms Al-Guneid: No, thank you. That was comprehensive. I wanted just to understand the real impact here, so thank you.

The Chair: Okay. Thank you very much.

Any other questions?

Okay. Thank you, Ms Ball and Ms Briggs, for your presentation and joining us here today. You are free to carry on with your day; however, you can remain on the videoconference if you want to observe. If you prefer, you can exit the videoconference if you want to go on with your day. Thank you very much.

Okay. We will now move to the privacy commissioner panel. First of all, I would like to acknowledge that Commissioner Harvey, Commissioner Dufresne have travelled from Victoria and Gatineau, respectfully, to be here in person to present to us today. On behalf of the committee I'd like to thank you for putting in that effort and coming all this way.

We will start with Commissioner McLeod's presentation. Please introduce yourself and your staff. You will have 15 minutes. This is for Alberta. Thank you. Go ahead.

Office of the Information and Privacy Commissioner of Alberta

Ms McLeod: Thank you very much, Chair. I am here today with my two assistant commissioners, Cara-Lynn Stelmack and Chris Stinner, and of course I'm very pleased to have my colleague commissioners here from the federal side of the equation and British Columbia.

With that, I will start my presentation. First of all, thank you very much for the invitation to be here today. I am pleased to have the opportunity to address you today as you continue your work on the review of the Personal Information Protection Act. I am also pleased that you are hearing two other important perspectives on PIPA from the Privacy Commissioner of Canada, Philippe Dufresne, and the B.C. Information and Privacy Commissioner, Michael Harvey. I thank them for being here.

10:00

Updating and strengthening PIPA is critical to the advancement of Alberta's interests. Since PIPA came into force more than two decades ago, the state of technology and the amount of personal information shared with organizations by individuals has changed monumentally. Dramatically expanded use of cellphones, apps, social media, online shopping, and more means that technology touches everything. Vast amounts of personal information are collected, used, and disclosed by private-sector organizations. Artificial intelligence, or AI, is ushering in even more changes, including effects on education and children. This has immense potential benefits for society but also great potential for harm.

PIPA needs to be amended to protect Alberta's privacy while also enabling commerce especially related to the development and use of innovative technologies. Alberta needs a modernized private-sector privacy law that aligns with leading global privacy laws and achieves balance between protecting privacy and enabling the use of technology by businesses seeking to prosper.

I want to first note the strong case for harmonizing PIPA with other access and privacy laws within Alberta and nationally. I noted in my review of stakeholder responses that this was a common theme. This harmonization is important to many jurisdictions and to businesses that want certainty in this respect. It is especially important for the continued cross-border transfers of personal

information to conduct business and for organizations that must meet the requirements of more than one of our privacy laws in Alberta. This includes the need for privacy law to apply to all organizations in the province that collect, use, and disclose personal information, including nonprofits and political parties, to ensure that there is a strong foundation of privacy protection across the province in all sectors. This will also enable Albertans to understand their rights, regardless of activity in Alberta.

Modernization and harmonization of privacy laws around the world means taking a stronger, rights-based approach. This will facilitate the ability of organizations to collect, use, and disclose personal information for purposes beyond ordinary business transactions and will allow them to innovate and participate meaningfully in the digital economy.

Currently PIPA balances rights against reasonable collection, use, and disclosure of personal information. Within this environment balance can only be achieved by increasing rights if amendments to PIPA increase the authority of businesses to collect, use, and disclose personal information in order to innovate. Rights must correlate to the digital economy and innovation, including for the use of AI. Looking around the world, modernized privacy laws include the General Data Protection Regulation, which is Europe's data privacy law; the Consumer Privacy Protection Act, which is part of Bill C-27; B.C.'s revised PIPA and Quebec's privacy law, known as QL-25; and laws in California, including the California Consumer Privacy Act.

The common rights that are recognized by these laws include the right to be forgotten, the right to data mobility and portability, rights around automated decision-making, and children's privacy rights. These are rights that a modernized PIPA should recognize in a growing digital economy.

A modernized PIPA in Alberta must also address the inevitable risks being created by the growing and expanded use of technology. This should include increased protections for processing sensitive information, including biometrics and personal information of children, and the prohibition of certain activities related to children. A failure to provide compensating rights and protections within a new PIPA could lead to the erosion of public trust, and this could mean the consequent failure of business and technology innovation, which relies on that trust. Effective participation by Alberta businesses in the digital economy relies on increased collection, use, and disclosure of personal information. This cannot be achieved without a strong foundation of public trust in the businesses and organizations that hold personal information.

How do we ensure a foundation of trust? Through the creation of a responsible innovation framework within a modernized PIPA. What should such a framework include? Clear definition about what personal information is considered to be sensitive and commensurate controls and obligations, requirements for privacy management programs, requirements for privacy impact assessments for certain high-risk processing activity, enhanced safeguards to secure personal information, requirements for communications and notices in plain language, requirements for compliance and accountability by service providers and downstream service providers, ethical obligations, modifications to requirements for mandatory breach notification that expedite notice to affected individuals.

The creation and maintenance of an environment within Alberta to allow for innovation relies on changes to PIPA that support such innovation. At the same time PIPA must mitigate as much as possible the risks and negative effects of technologies and practices used in innovation. PIPA should include limitation principles that require the use of anonymized personal information wherever possible, followed only by the use of deidentified personal information and only personal information if necessary; definitions and standards for what constitutes deidentified personal information and anonymized personal information; the ability to use personal information in a controlled environment to create deidentified or anonymized personal information and to create synthetic data; prohibitions on reidentification of deidentified personal information; restrictions on specified uses of personal information such as for the development of innovative technology, including for training AI; and effective oversight of these activities. Effective oversight is essential to promote, support, and assess or audit compliance and to deter noncompliance through financial penalties that are designed to encourage compliance and that are not punitive.

A modernized PIPA will necessarily contain provisions to encourage support and enforce compliance. The way our new PIPA is drafted in this regard is of key importance. The new legislation should require more and more rigorous security measures when the privacy risks are higher and fewer and less complex security measures when the risks are lower. In other words, compliance measures should be scalable according to what activities are being undertaken with personal information and what the risks are. This can be assessed according to the degree of sensitivity of personal information, the amount of personal information being handled, the nature of the processing, and the potential for harm. Such scalable compliance measures would help achieve two important policy objectives: one, to avoid placing an excessive compliance burden on small businesses or other organizations that do not rely on the collection, use, and disclosure of personal information or sensitive personal information; and, two, to give Albertans greater assurance that their personal information is given greater protection where it matters most.

Now is the time to modernize PIPA. Alberta is already an innovation leader in Canada. Our privacy laws must be amended to facilitate continued innovation, leadership, and prosperity while adequately protecting the privacy rights of Albertans. We must not wait. The time is now to harness the benefits of using innovative technology while also protecting privacy rights. If we follow the general approach to modernization being taken by the federal Consumer Privacy Protection Act in Bill C-27, we will be in line with provincial, national, and international laws. The modernization will ensure Alberta is placed as a leader with a made-in-Alberta privacy law that serves progress in the digital economy in the province. It is time.

Finally, a note about what everybody is talking about, and that's AI. Regulation of artificial intelligence is necessary to mitigate harm. The use of AI should be regulated in Alberta, regardless of whether personal information or health information is involved. Because AI is changing and evolving rapidly, there is a critical need to implement guardrails for the development and use of this technology in order to adequately protect Albertans from harms that may flow to them from these activities. We would be pleased to discuss our views on how this can occur in Alberta to promote responsible innovation.

I will conclude by saying that PIPA legislation needs to be designed to ensure that Alberta's economy and services to Albertans can thrive while at the same time ensuring organizations and businesses protect the rights and privacy of individuals. Thank you again for the opportunity to provide my comments here today, and I look forward to any questions that you may have.

The Chair: Thank you, Ms McLeod.

Next I would like to invite Commissioner Harvey from British Columbia to make your presentation. You have 15 minutes. Please introduce yourself and begin when you're ready.

10:10

Office of the Information and Privacy Commissioner for British Columbia

Mr. Harvey: Thank you very much, Chair, Deputy Chair, members of the committee. My name is Michael Harvey. I am the Information and Privacy Commissioner for British Columbia. It is a real pleasure to be able to have the opportunity to speak to you today and to join my colleagues. We are a close group of colleagues around the federal-provincial-territorial commissioners' table, and it's really important that we can support each other but also to talk about the important harmonization of our laws.

I would first like to acknowledge and respect that we are meeting this morning on traditional Treaty 6 territory and within the Métis homelands and Métis Nation of Alberta region 4. I'm honoured to present to you on this land today.

Thank you for inviting me to appear today as part of your review of the Personal Information Protection Act. Like our own legislation in B.C. of the same name, PIPA protects the privacy of individuals while enabling the use of personal information for business to prosper. I will focus the majority of my remarks this morning on two specific areas where British Columbia's act differs from the Alberta legislation, specifically oversight of political parties and of nonprofits. Harmonization between the two jurisdictions in these sectors would be beneficial, especially to those organizations that operate in multiple jurisdictions and for those they serve. While the two acts are very similar, we looked at the strengths of each other's laws. For example, we have used Alberta as a case study for the need to implement mandatory breach notification for the private sector in British Columbia, and I hope that the additional protection British Columbians received is valuable for your discussion and deliberations.

But, first, I will speak to the importance of strengthening the act specifically with a mind to children by providing the Information and Privacy Commissioner with stronger enforcement mechanisms such as monetary penalties for more effective oversight. The matter of protecting and promoting the information and privacy rights of young people in the digital world is a matter that this office, my office, has advocated for both in British Columbia and at the federal level and has seen numerous calls from other regulators around the world.

Our children are particularly vulnerable to overcollection of their personal information online. We know that our kids spend much of their day online, whether interacting with their friends, playing games, or completing their schoolwork. We also know that children are often the target of deceptive design practices used by websites and apps that manipulate our kids into revealing their private information or by causing other harms. In a recent review conducted by privacy regulators around the world, we found a higher incidence of these manipulation tactics in Canada than in other countries, yet we still don't have adequate protections in this country that address the specific challenges and unique harms our youth face when they engage online.

And it isn't only parents and regulators that have voiced concerns. We know both from conversations at a youth forum that the B.C. OIPC held in 2023 and through the research of others that youth care about their information and privacy rights online, and they put considerable effort into protecting their rights by using various privacy protective strategies such as limiting who can view their social media posts and talking about consent in digital spaces online, but it's not enough. As legislators there is an urgent need to address the shortfalls by enhancing the enforcement mechanisms available to regulators for greater oversight over organizations that provide products and services to children.

We have recommended to the government and Legislature in B.C. that the commissioner be given authority to issue stronger fines for organizations that don't honour their obligations under the law. We call these administrative monetary penalties, or AMPs, and while they are an important tool across the board, they will be the most important enforcement authority that we could use to help protect children and youth.

As a regulator, we have always emphasized an educational, remedial approach to compliance. We work with organizations to achieve compliance through recommendations and findings wherever possible, and this approach works much of the time, but the reality is that there are some entities that just don't follow the rules. Introducing monetary penalties would introduce an appropriate level of deterrence with penalties reserved for the most serious violations of the law, and the range of penalties should be proportionate based on the offence.

I can inform this dynamic from the other hat that I wear. In B.C. as commissioner I am also designated the registrar of lobbyists. In that role I have the authority to levy penalties when a contravention of that statute has occurred. We lead with education. It is the best way to support compliance with the act and therefore its overall purpose. However, the ability to levy penalties plays an important role in incentivizing the willingness to comply, particularly in cases where there is, let's say, little interest in following the rules set out under the law.

Other shortfalls that should be addressed when it comes to children and youth include strengthening protections around consent requirements and making sure that privacy policies are in clear and plain language. This could include containing language suited to the age of the child.

We recommended these measures to our own review committee in 2021, and the special committee agreed by including the recommendations in their report to the B.C. Legislature. Taken together, these measures provide a path for holding organizations to account in putting the best interests of the child as a primary consideration when designing and developing online products and services that children are likely to use. The importance of addressing children's rights in our privacy legislation is recognized across Canada, and I expect Commissioner Dufresne will provide you with some more information about the developments happening at the federal level.

I will now shift my comments to two sectors that are not covered by Alberta's PIPA but are covered in British Columbia, political parties and the nonprofit sector. In January we celebrated the 20th anniversary of B.C.'s PIPA, a significant milestone for our private-sector privacy law. Since its inception political parties have been subject to the legislation. That means that in B.C. voters can expect the same privacy protections from political parties as other organizations and have an independent body, the OIPC, to which they can make a complaint if they have concerns about a political party's privacy practices.

B.C. PIPA applies to the collection, use, and disclosure of personal information by B.C.'s political parties in the same way that PIPA applies to other organizations. In other words, there aren't specific rules set out for political parties; rather, they must follow the same requirements as any other organization in B.C. This means that the rules of PIPA apply when political parties directly approach voters to collect personal information about them such as door-to-door or telephone canvassing or when they indirectly collect personal information such as on social media or from prescribed sources of public information. As well, PIPA requires parties to inform individuals about the party's privacy practices through

privacy policies and provide access to individuals' own personal information. There are also rules on consent, notification, collection, and reasonable purpose.

I can state unequivocally that our political system has not collapsed as a result of PIPA applying to the practices of political parties; quite the opposite. A functioning democracy is predicated on political parties understanding the aspirations of voters and communicating with the electorate, communication that very often includes personal information about voters. The application of privacy laws to political parties is essential if voters are to have confidence in how political parties process the vast amounts of personal information that they collect about individuals. Without a privacy framework in place, communications between candidates and the electorate can be frustrated, and nobody wins.

Provincial political parties in B.C. – I won't comment on federal parties, as that is before the courts – have committed to upholding these protections for the citizens of British Columbia. In 2022 the parties that were represented in the Legislature at that time voluntarily signed a code of conduct that detailed how PIPA will be applied in their context. Our interaction with parties in the run-up to this election has been positive and constructive. Privacy oversight is working and working in the interests of the people of the province. To echo the calls that the federal, provincial, and territorial Canadian privacy commissioners have made now on multiple occasions, all Canadians deserve the protections that British Columbians have enjoyed for the last two decades.

Finally, I'll turn to the importance of capturing not-for-profit organizations under private-sector privacy legislation. Since its inception our B.C. PIPA has also applied to nonprofit organizations, including trade unions, charities, foundations, trusts, clubs, churches, and amateur sports organizations. Like political parties, there aren't specific requirements directed at nonprofits; rather, they are required to follow the same obligations as other organizations.

I can say that it is difficult to come up with a convincing justification for excluding nonprofits from the requirements of our privacy law. Think for just a minute about the work that they do and the vast amounts of personal information, sometimes sensitive, that nonprofits potentially hold: information about donors, clients, volunteers, children, and many times dealing with vulnerable populations.

10:20

We expect this information to be protected in the same way as with other organizations and that, should a breach occur or if individuals have concerns about how their personal information is handled, there is a process in place and an oversight body to report it to.

To give you an idea of the types of nonprofits we have dealt with under B.C.'s PIPA, we often have consults with sports organizations and nonprofits that work with other public bodies; for example, to assist the unhoused or help respond to the opioid crisis. PIPA is not a burden to these organizations. Rather, it provides them with the rules and guidance to follow to gain the trust of those they serve. It provides them with my office as a resource when needed, either for a consultation or to provide guidance when dealing with personal information, and it gives the people who volunteer, donate, or interact with nonprofits assurance that there are laws in place to protect the sometimes very sensitive personal information nonprofits can hold and a mechanism when those rules aren't followed.

I can share from my experience in my previous role as commissioner in Newfoundland and Labrador, where we did not have oversight over nonprofits, that we would regularly receive inquiries from them seeking our support and training, and we would regularly advise them on the privacy principles that inform our laws and best practices. Generally the sector there was looking for the guidelines that our regulatory framework provides.

Thank you, Chair and members of the committee, for your attention this morning. I look forward to answering any questions that you have.

The Chair: Thank you, Mr. Harvey.

Finally, we will hear from Commissioner Dufresne, representing the Canadian commissioner. You have 15 minutes. Please introduce yourself for the record, and you may begin.

Office of the Privacy Commissioner of Canada

Mr. Dufresne: Thank you. Philippe Dufresne, Privacy Commissioner of Canada. Very happy to be here. Good morning, Mr. Chair, members of the Standing Committee on Resource Stewardship, for inviting me to offer my observations for your review of Alberta's Personal Information Protection Act. I'm pleased to have this opportunity to highlight the context of federal privacy law reform and how the interoperability of privacy laws benefits both consumers and businesses. In May I provided a written submission to your committee, which will form the basis of my remarks today.

I want to begin with an overview of my role. As Privacy Commissioner of Canada my mission is to protect and promote individuals' fundamental right to privacy. This includes overseeing compliance with both the Privacy Act, which applies to federal public institutions' collection, use, disclosure, retention, or disposal of personal information, and the Personal Information Protection and Electronic Documents Act, or PIPEDA, which is Canada's federal private-sector privacy law.

We live in a rapidly expanding environment of emerging technologies and business models that leverage the use, collection, and disclosure of personal information. These advances bring many benefits for our lives, for the economy, but they also introduce new privacy risks that make protecting privacy more important and challenging than ever.

The three pillars of my vision for privacy, which I outlined at the beginning of my mandate two years ago, reflect this environment. They are: one, privacy as a fundamental right; two – and this is relevant to this discussion on balancing small businesses and innovation in the economy – privacy in support of the public interest and Canada's innovation and competitiveness; and, three, privacy as an accelerator of Canadians' trust in their institutions and in their participation as digital citizens. These pillars reflect the reality that Canadians want to be active and informed digital citizens and should not have to choose between this participation and their fundamental right to privacy.

These pillars are woven into the strategic priorities that I announced earlier this year and that will guide the work of my office for the next three years. The priorities are: one, maximizing the impact of the OPC and my office and fully and effectively promoting and protecting the fundamental right to privacy; two, addressing the privacy impact of new technologies, including generative AI; and, three, championing children's privacy rights.

My strategic plan includes investment in partnerships and joint initiatives with provincial and territorial data protection authorities. I am so proud and grateful for the excellent relationship with my provincial and territorial counterparts and for the close collaboration with Commissioner McLeod and the office of the Information and Privacy Commissioner of Alberta as well as Commissioner Harvey and the Office of the Information and Privacy Commissioner of British Columbia.

Canadians need and expect modernized privacy laws that support innovation and enable them to enjoy the benefits of technology with the reassurance that their personal information is being protected. The interoperability of privacy laws, both domestically and internationally, is a key factor in that assurance. It is essential to fostering Canadians' trust that their personal information will be protected no matter where their data resides or is transferred. Interoperability also benefits organizations as it can simplify regulatory requirements and reduce compliance costs. This facilitates innovation and competition for Canadian businesses, and organizations benefit from the clarity that is provided by joint regulatory guidance. I've heard this in Canada; I've heard this across the world.

PIPEDA sets national standards for privacy practices in the private sector, but organizations may be exempted from the application of PIPEDA with respect to the collection, use, or disclosure of personal information that occurs within a province where a provincial law that has been deemed to be substantially similar to PIPEDA applies. Alberta, Quebec, and B.C. currently have private-sector privacy laws that have been deemed substantially similar to PIPEDA. This means that in many circumstances the provincial law applies instead of the federal law.

Having substantially similar laws allows me to work closely with my counterparts in Alberta, Quebec, and B.C. on activities such as joint investigations and guidance for organizations to help them with compliance. My colleagues and I have a memorandum of understanding that sets out a framework to support collaboration to leverage resources, increase knowledge sharing, and ensure consistent and effective, efficient oversight of private-sector privacy in Canada. Joint investigations have included cases such as Clearview AI, Facebook, Cambridge Analytica, with a recent decision of the Federal Court of Appeal in the last two weeks, Tim Hortons, and, more recently, OpenAI and TikTok as well as another ongoing investigation into a company that offers background check services, including tenant screening services to landlords. We've also worked together to draft joint guidance such as our principles for responsible generative AI technologies, which we issued last December.

I also place a very high importance on forging international partnerships, recognizing that interoperability and harmonization at the global level is important to facilitate commercial exchanges of personal information across borders. In January of this year Canada's adequacy status under the European Union's GDPR, General Data Protection Regulation, was reviewed, with the European Commission finding that Canada continues to provide an adequate level of protection of personal information transferred from the EU to recipients subject to PIPEDA. In its report the European Commission recommended enshrining in legislation some of the protections that have been developed at the sublegislative level, so guidance documents and recommendations from my office and others, to enhance legal certainty and consolidate new requirements such as requirements for sensitive personal information. The commission noted that it intends to closely monitor future developments in Canada.

Next month I will meet with the Roundtable of G7 Data Protection and Privacy Authorities, my fellow privacy commissioners from G-7 countries. We've been gathering since 2021 to discuss regulatory and technology issues and developments and have issued common positions. For example, last year in Tokyo we released a joint statement on generative AI under the Japanese DPA presidency. The group has committed to working together to foster future interoperability where possible in order to achieve a higher level of data protection and facilitate data free flow with trust. Next year, as Canada assumes the G-7 presidency, I will take on the presidency of the Data Protection and Privacy Authorities Roundtable, and I look forward to hosting my G-7 colleagues in Ottawa and helping to advance important collaborative initiatives during Canada's presidency.

Other examples of international co-operation include this year's global privacy enforcement network sweep, where the OPC was one of 25 privacy authorities from across Canada and around the world that reviewed more than 1,000 websites and mobile apps. We found that 97 per cent used one or more deceptive design patterns that could influence individuals into giving away more of their personal information online. My office also helped to lead the drafting of a statement on data scraping with members of the Global Privacy Assembly's international enforcement working group last year. This statement prompted an instructive dialogue with some of the world's largest social media companies and included a reminder that information on the Internet is still subject to privacy laws in most jurisdictions.

10:30

Another global privacy assembly working group which I chair recently launched an international privacy and human rights award. This award will celebrate exemplary work by an individual or organization to promote and protect privacy and other fundamental rights. The inaugural award will be presented at the 2025 RightsCon conference in Taipei in February.

On June 16, 2022, the government of Canada tabled Bill C-27, which would repeal part 1 of PIPEDA and enact the CPPA; the Personal Information and Data Protection Tribunal Act; and the Artificial Intelligence and Data Act, or AIDA. The bill has been going through clause-by-clause consideration by the House of Commons Standing Committee on Industry and Technology, which we call INDU. Bill C-27 would maintain PIPEDA's approach to substantial similarity. As is the case under PIPEDA, the Governor in Council would determine whether the privacy legislation of a province is substantially similar to the CPPA. Under C-27 the Governor in Council would also make regulations establishing the criteria and process for making or reconsidering a determination of substantial similarity.

In many ways Bill C-27 is an improvement over PIPEDA. It establishes stronger privacy protections for individuals and creates incentives for organizations to comply while allowing for greater flexibility to innovate. Encouraging innovation in a privacy protective manner will help increase individuals' privacy and control over their personal information as well as their trust and ability to realize the benefits of the online economy.

In April 2023 I made a submission on Bill C-27 to INDU with 15 key recommendations that I believe are necessary to better protect the privacy of Canadians while supporting Canada's innovation and competitiveness. I would note that my submission on Bill C-27 discussed many of the topics that are raised in the document that was posted by this committee entitled Emerging Issues: The Personal Information Protection Act. These include consent, the identification and anonymization, privacy impact assessments, administrative monetary penalties, automated decision-making, the right to erasure, and data portability.

I'm pleased to offer some detail about these recommendations as considerations to support your review of Alberta's PIPA. For instance, in the submission on Bill C-27 I recommended expanding the list of violations qualifying for financial penalties to include violations of the appropriate purpose requirement, which is a key element of privacy protection. I also recommended requiring organizations to build privacy into the design of products and services and to conduct privacy impact assessments, or PIAs, for high-risk activities. PIAs can help organizations demonstrate that they're accountable for personal information under their control,

ensure that they're in compliance with the law, and limit the risk of privacy breaches. In my October 2023 parliamentary committee appearance on Bill C-27 I also highlighted PIAs as a particularly critical measure in the context of artificial intelligence and other high-risk initiatives that may have a significant impact on individuals.

Achieving commercial objectives and privacy protection are not mutually exclusive. I often talk about rejecting the zero-sum game between privacy and protection and innovation of public interest. Privacy can be an accelerator of Canadians' trust in the digital economy rather than an obstacle to innovation and competition. However, in those rare circumstances where the two are in unavoidable conflict, fundamental privacy rights should prevail. This is why my first recommendation with regard to Bill C-27 was to recognize the fundamental right to privacy in the law in both the preamble and purpose clause of the CPPA and to embed the preamble in the acts that would be enacted. I was pleased to see the INDU committee reflect this recommendation, adopting an amendment to that effect.

Another of my key recommendations was to amend the preamble to recognize the importance of children's privacy and the best interests of the child. INDU has also adopted this recommendation. Including the best interests of the child in the preamble will encourage organizations to build privacy for children into products and services from the start and by design and serve as an important interpretive tool. The addition of children's privacy to the framing section of the legislation is especially encouraging as it reflects the recommendations made in the resolution of the federal, provincial, and territorial privacy commissioners and ombuds with responsibility for privacy oversight on putting the best interests of young people at the forefront of privacy and access to personal information. I was proud to see this FPT resolution cited and commended by members of the committee, and this highlights the importance of our strong FPT collaborative work in promoting and protecting privacy in our jurisdictions.

INDU has also amended the bill to include definitions for lawful authority, minor, profiling, and sensitive information. They've also, notably, amended the definition of personal information to include inferred information. These amendments will help clarify organizations' obligations under the law. Clause-by-clause consideration of Bill C-27 continues, and I hope that INDU will continue to implement my recommendations and those of other stakeholders to strengthen the bill.

Your review of PIPA comes during a pivotal time for privacy law reform in Canada. I agree with Commissioner McLeod. It is time. Fostering consumer confidence in organizations' responsible use of personal information is critical in helping position Canada as a global leader in privacy. I believe that a strong, harmonized federal-provincial-territorial privacy regime based on common principles will help to achieve this goal, and I'm committed to continuing this important work with my colleagues Commissioner McLeod and Commissioner Harvey.

With that, I would be pleased to answer your questions. Thank you.

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

I'll now open the floor to committee members to ask questions of the three commissioners. We'll start with MLA Eggen. Go ahead.

Mr. Eggen: Thank you, Chair. Through you, I just wanted to ask Ms McLeod about her recommendations to changes to our privacy act here in Alberta and specifically if there's anything that you are recommending that is substantially different from what we see in British Columbia or other jurisdictions and then nationally as well. You've mentioned on more than one occasion that, you know, you want to have a made-in-Alberta solution to this, but, I mean, we're talking about harmonization here across the country, so, like, what are you suggesting that would be different from the national standards that are being set or provincial standards such as in British Columbia?

Ms McLeod: Great. Thank you very much. I would first say that most of my comments are framed around the framework that we have seen in the federal CPPA as well as the GDPR, which the CPPA is modelled after. In terms of, you know, what makes it an Alberta approach is the scalability in the application of the law to the various sizes of organizations that are within our province. PIPA was actually drafted to address the needs of small and medium-sized businesses in Alberta, and we have maintained that framework within the law, so that's what makes it a unique Alberta approach.

The other thing that I would add to that is that Alberta is very involved – I'm not sure if that's the right word, but leading the way in the development of artificial intelligence in Canada, and we need to have these laws in place to ensure we have those adequate guardrails. We have certainly emphasized some of that in the act, and as Commissioner Dufresne pointed out, in C-27 they have the AIDA legislation, which is the Artificial Intelligence and Data Act, and my recommendation includes having an Alberta similar kind of law to deal with intraprovincial artificial intelligence as opposed to data that is travelling across the border that may be subject to AIDA when it comes to those kinds of processing activities set out in that legislation.

Mr. Eggen: Okay. You know, my concern is that, of course, it's a very fluid situation – right? – the exchange of data between jurisdictions and indeed around the world. You know, if we have different protections or the lack thereof in any given jurisdiction or Alberta specifically, then, I mean, doesn't that put us at risk for people to know that and to take advantage of that if a particular jurisdiction like Alberta has different laws or rules around data and protections? I mean, doesn't that expose us to people taking advantage of that?

Ms McLeod: So if I understand your question, you're talking about, essentially, the security requirements in the legislation? Yeah. So we have recommended strong security requirements in our legislation, and even though we have identified things that are more specific to Alberta such as things that I just mentioned, we have certainly, I would say, recommended the best in class in terms of privacy protection in Canada. Taking models from Quebec, for example, is considered to be one of the gold standards in Canada right now. The CPPA has some very good provisions to strengthen Canada's privacy laws.

10:40

But we have actually, you know, taken the best in breed from not only Canada; the GDPR, California, and some other jurisdictions that are looking at these laws and modernizing their legislation, the goal being that Alberta will have a strong privacy law that is, at minimally, harmonized with our federal counterparts, British Columbia but also has more strength in it so that we can actually facilitate the innovation that's occurring in the province and ensuring that we have that adequate balance with the privacy protections. So it will not be weaker. If anything, as my recommendations exist, it would be stronger.

The Chair: Thank you very much.

Member Sinclair, go ahead.

Mr. Sinclair: Thank you, Mr. Chair. Thank you, everyone, for all your hard work and for the travel that both Commissioner Dufresne and Commissioner Harvey made here today and your team. Appreciate that.

Although I agree with some of the concerns from my colleagues here today on the committee regarding the proposed changes to PIPA and finding the balance between protecting citizens, their private information while not trying to overregulate to the point where it's a hindrance to small business or nonprofits, as a dad with two young daughters this is where my biggest concern lies specifically. It's for the commissioner of Alberta. As you stated in your report, the Internet has played an increasingly important role in children's lives despite the numerous inherent risks involved with accessing many web-enabled services. You explain that our current PIPA legislation does not offer any specific protections for children in terms of Internet use and that must be addressed in order to keep children safe across Alberta. Would you be able to outline some of the existing challenges PIPA has by not including specific information, privacy protection regarding children? I know you broadly mentioned a couple, but if you could be a little bit more specific, and if you don't mind defining what youth means specifically, if that's under 18, if you don't mind.

Thank you.

Ms McLeod: Thank you very much for the question. I'd just like to state here that I acknowledge the hard work that this committee is faced with. I don't think I've ever seen a time in the history that I've been involved in privacy, which dates back to the '90s, where we are in an environment that is so complex. We are in such a technology-driven environment, and the technology is increasing. To your point, the children are being exposed to risks that they're not even aware of, the parents aren't even aware of, the deceptive practices that are occurring through – I'll use some examples. Social media is an example of it.

Another thing that's important to remember is that PIPA actually regulates beyond Alberta's borders, so if information is collected in Alberta, that organization must comply with our rules. If we're talking about Alberta children, then we need to be thinking about the organizations outside of Alberta's borders that are affecting our children.

Commissioner Dufresne talked about a sweep that we did earlier this year. Alberta participated in that as well. We did find that there are a number of deceptive practices that actually influence children in a number of ways. We focused on things like privacy policies, trying to obtain additional information, the ability to opt out. It's all very difficult, and that's why the right to be forgotten is also an important right here because if you think about when our children went on the Internet – I think mine were in their teens at the time – you know, some of our kids have just grown up and they put all kinds of data out there, and they need to have some rights to protect them.

But we also need to impose rules on these big organizations that are using our children to manipulate them into different things, to ensure that protection exists. That's why the commissioners are calling for protections to be codified in legislation to ensure that these organizations will be held accountable for those kinds of practices. My commissioner colleague also talked about administrative monetary penalties. Again, those are intended not to be punitive but certainly to hold someone to account where they're engaging in egregious activity that may affect children, for example, and cause harm.

Your last question was about the age. That's a tricky one. I've done some reading on what they think an appropriate age is. Sometimes it's under 13 to prevent the collection of information, between 13 and 15 with certain parental consent, and between, I think, 15 and 18 with some other controls in order to control what those organizations can do as it relates to our children.

The Chair: A follow-up?

Mr. Sinclair: Yes. Would you be able to expand on some of the considerations put forward in your report to the committee on protecting children's information, and what are some of the national or international policy legislations these considerations are based on or perhaps interprovincial here with the colleague to the left of you?

I will just say that personally I appreciate the work. Again, as a parent we are all guilty of it, I think, raising kids right now with them having too much screen time, but trying to monitor what it is that they're doing. Yesterday I played my first game of Roblox with my daughter. I don't like that game; they love it. I found myself a little bit concerned. She's only eight years old, and she made a reference to Louis Vuitton in regard to one of the bags in some game we were playing, so I think these concerns are real. We definitely need to continue this work, and I appreciate it.

Thank you.

Ms McLeod: Yeah. I'm going to let my colleagues talk about this a little bit. The work that I put into my recommendation stemmed largely from the work of the federal office, so I think I'll let them speak to that. But I just want to comment on a point you made that when these social media apps came on and/or the gaming, because, you know, kids all game, too, as well, we didn't realize what was happening. Now we're learning what's happening, and also these organizations are monetizing the information in a way that potentially has the risk of harm. Everything is evolving, but now is the time that we need to add that protection.

I'm going to pass it over to my colleagues to speak to it a little bit.

Mr. Dufresne: Thank you. Certainly, Bill C-27 has highlighted the protection of minors as being an important element, and we've strengthened that by recommending the recognition in the preamble and the importance of the best interest of minors. Concretely, what the law would do is that it recognizes that minors' personal information is deemed to be sensitive, so that impacts a number of obligations for: how do you obtain consent; how do you communicate; how do you treat that information, how do you protect it?; giving more rights to kids to request the deletion of their information that may have been collected when they were a minor and now they may realize: I don't want that to be available anymore. So there are some concrete legislative tools that we need to be stronger in that sense.

Now, we're using the tools that we have. We've issued the statement across our jurisdictions calling on organizations: "Here's what you need to do. You need to be more clear. You need to have the best interests of the child at heart." That's an internationally recognized norm; it's a norm recognized in our case law in our courts. We warn against those types of deceptive practices. Sadly, our sweep this summer, that we did together with Alberta and others and with colleagues around the world, showed that not only the mainstream organizations were using these deceptive tools to manipulate all of us into giving our consent but also sites geared to kids, so that's even worse. They're more vulnerable. They need more protection.

Another concrete area where kids' protection comes into play with privacy is the whole issue of age assurance, age-appropriate codes and guides. So we're working on that to see: how do you protect kids online, not only their privacy but protect them from

abuse and hate and sexual violence and all those things? Age verification raises issues of privacy, so we've launched a consultation nationally on this to provide recommendations, and we've issued with international partners a statement just a few days ago highlighting some of those principles.

Ms McLeod: I would just like to add one thing before I pass it over to Commissioner Harvey. We actually used the education apps being used in Alberta by the public school system as our focus, and we found those same deceptive practices.

Mr. Harvey: MLA Sinclair, I think you've brought a really important perspective to this conversation that resonates with so many of us that are parents, but also every one of us, whether we're parents or not, has connections to children. You know, I was in that situation with my kids playing Roblox some years ago, and the concern that I faced when I saw them playing Roblox was that they were overhearing conversations with much older people that were quite inappropriate. So in that situation as a parent – I'm not talking about here as a regulator; I'm talking as a parent – we put the block on Roblox at that particular time because of the specific incident of them hearing interactions with other people, strangers.

That's not a privacy matter, but the broader issue of our children online is something that has really taken the world by storm, not just in privacy circles but broader. For example – and again this is outside of our specific mandate – across the country education systems have brought in limitations on the use of smart phones in schools. This has been triggered in large part by a book, that I really encourage people to read, written by a psychologist called Jonathan Haidt called *The Anxious Generation*, in which he explores the relationship between mental health and our children who have grown up during the smart phone era.

10:50

The connection to privacy here may not be exactly obvious, but I want to take a moment and draw to it because I think it's really important and it speaks to that a deeper understanding of privacy is necessary for understanding where our kids are and understanding why these deceptive design practices are so important. We often might think about privacy as how to take information about you and put it in a box and keep it safe and not accessible by unauthorized actors. I encourage you to think about privacy more broadly as about control, how we in this world control the information about ourselves, about how we exist in this society as an autonomous and dignified individual. That's what a rights-based approach to privacy means.

Now, we say that our children are growing up in an online world. The online world is to the point where talking about online is irrelevant now. Our whole world is online. As we speak, our information is being, you know, shipped around the world. I can see it shipped around the world in front of me. Our children are being raised in this environment, and their identities are being shaped in their environment, so when we talk about the privacy of our children online, we're talking about their very identity formation. They're going through, they're living in this world at the same time, at that critical part of their lives when they're forming their identities. So if they're being exposed to uncontrolled deception and manipulation at a time when their identities are formed, that is why we're seeing the relationship between an increase in screen time and mental health issues.

This is fundamentally important for the future of our society. The task ahead of you, as Commissioner McLeod has said, is one of enormous and kind of existential importance for the future of the society here in Alberta and across the country.

The Chair: Okay. Thank you very much.

Our next question comes from Member Al-Guneid. Go ahead.

Ms Al-Guneid: Thank you, Chair, and through you, thank you all for being here. I do appreciate all your presentations. I found them comprehensive and interesting. Commissioner Harvey, I do relate to your comments as a parent. As MLA Sinclair shared, it's tough having these conversations as well, as a parent with children.

I want to go back to questions I asked earlier. I'm not too sure if the panel was present when I shared my previous questions, but I'd like to reiterate that the United Nations Secretary-General's advisory body published a report on AI frameworks arguing that AI regulation at the local and national levels has been problematic and, therefore, a global regulatory framework for AI is essential. As you can see, the UN sees this as a global issue with a global approach. You kind of talked about this in all your presentations. I think you see that we don't have room for a fragmented approach by the provinces. It requires a national approach. I was glad to see the Privacy Commissioner of Canada mentioning joint efforts and joint conversations with Alberta and B.C.

My questions to the panel: how does this look actually in practical terms? How are Alberta and B.C. governments working with the government of Canada on AI regulation in practical terms? I understand that AIDA is under consideration right now, but can you share a couple of examples on what that would look like? That's my first question. Then, two: what is the government of Canada doing at the moment to integrate the UN's AI framework, and also what areas of the GDPR is the government considering? As I mentioned earlier, in the LinkedIn development right now EU citizens are better protected today than all of us here in Canada because of GDPR.

And then, finally, a question to Ms McLeod. You mentioned that AI needs to be regulated, and I do agree with you, and I'm happy to hear your comments on that and specifically on the right to be forgotten. I believe your submission mentions that AI regulation is beyond the scope of PIPA, so can you please tell us more: how do you see the implementation of AI regulation in Alberta? So that's one. Second, you mentioned the scalability a few times. How can the compliance measures be scalable? I might have missed your comments there, so if you can please just give me a quick summary of what you meant there.

Thank you. A lot of questions there.

Ms McLeod: Okay. Thank you. I wasn't sure how many questions were in there, but did you want to hear about the federal work at the UN level? I think my colleague Philippe might be better to speak to that, and then maybe after that I can come back and answer those questions that you just asked.

Ms Al-Guneid: Yeah. My first questions were for the panel, and then just two specific questions to you.

Thank you.

Mr. Dufresne: Thank you. Very briefly – you're absolutely right – this is a world-wide issue; it requires a world-wide effort. This is why there is so much collaboration within Canada and outside of Canada, and AI is the perfect example on that. Last December we hosted in Canada a technology group, subgroup of the international community, to talk about AI. We invited leaders of industry, we invited colleagues from around the world, and we invited FPT commissioners to have a privacy symposium on AI, and that's when we launched our made-in-Canada principles for AI, which were noticed and which help the international efforts in this respect. In Tokyo last year with my colleagues the G-7 commissioners we issued what I think was one of the first international statements on

AI saying that privacy law governs AI right now. We need specific laws, we need modern laws, but we already have laws now, and we're using them.

This is why, with Commissioner McLeod and Commissioner Harvey, we launched the investigation on OpenAI, to test the compliance with our current laws. Again, there we were one of the first in the world. We issued internationally a joint statement on data scraping – very, very relevant – talking about social media companies. You have things online about your users. There's a lot of data scraping to train AI models and so on. What are the responsibilities; what is the best advice? We're using all of the tools at our disposal.

Specifically, the treaty that you're referring to, that's entered into by states and by government, would involve the government of Canada. I can't speak on behalf of the government of Canada because I'm an independent agent of Parliament, as are my colleagues, but I know that the government of Canada is involved in those discussions, that the Department of Industry is involved at the OECD level. So what I can say is that, certainly, we're looking at all of our tools and the collaboration. This is why I'm meeting my G-7 counterparts in two weeks in Rome to talk about this, talk about: how do we regulate AI? What's the role of the government? What's the role of the Privacy Commissioner? So this is a completely collaborative effort on all fronts.

Ms Al-Guneid: If I might add that the data deletion is the sticky point right now with generative AI. My data is baked in, just like sugar in a cake. There's no way for us to delete. Like, right now we can ask the LinkedIns and the Facebooks of the world to delete our data, and they would because that's our ask, but if you read their new privacy rules that they shared last week and two weeks ago, it's a different type or treatment of data, and it's impossible to delete them. That's what I'm curious about in the considerations and the conversations you're having with your counterparts and also at the global scale.

Thank you.

Mr. Dufresne: I'll just say briefly that, certainly, deletion of data in the context of AI is something that we're all thinking about in the context of guidance, in the context of investigations. So it's a live issue, for sure.

Ms Al-Guneid: Thank you.

Mr. Harvey: If I could add just some thoughts to this conversation. First of all, the issue of "how do you untrain an algorithm?" is a really, really important and complicated one, but it's also one that we will be dealing with – there's no question – in the coming months and years. All the more reason for us to really put our foot on the gas when it comes to developing appropriate guidelines and strengthening guidelines for AI now so that we don't in two to five years' time end up trying to have to put it to tech companies. How are you to tell them? How do you untrain an algorithm?

11:00

I also want to raise, I think, something that has been a little bit of subtext and at times text: concern about the fragmentation. Does developing, let's say, a made-in-Alberta approach or a made-in-B.C. approach risk creating a fragmented regulatory landscape with respect to AI given that action is required on a global level? I think that's an important question. But I think the answer is that this is an all-hands-on-deck moment. You're right, I think, to identify this as a risk, but the response to it is not to wait for that global silver bullet but rather to proceed as we can within the jurisdictions that we can with an eye towards harmonization and collaboration as we do that.

I also just want to comment on – I'm relatively new as commissioner in British Columbia and therefore new to the subset of our privacy commissioners that have private-sector privacy oversight. Now I've become involved over the last five months in our engagement on, for example, the enforcement action that we're doing on OpenAI, as Commissioner Dufresne has referenced. It is my view that it is not a weakness that there are four of us, including our Quebec colleague, around that table. It is a strength. When we get together and we debate the issues involved in that enforcement and tease them out and discuss it amongst each other, I am convinced that the outcome of that will be a more sophisticated and more appropriate outcome than if there was just one of us involved. There is not fragmentation around our table. There is strength in numbers. We contribute to each other with our ideas and find that strength in diversity.

I think it's important to ask those questions, but I think that Canada and our federation is based on our diversity. That is our strength. That's what makes us the best place and the best country in the world, so I encourage you to consider that as you move forward in PIPA reform.

Ms McLeod: Okay. Thank you.

Ms Al-Guneid: Thank you. Sorry. Just a quick comment on that. I do appreciate that perspective, Commissioner Harvey, and I do agree with you that we can't wait until the whole globe agrees on one thing. It's more about sharing best practices, and GDPR is already in action. I think one of you mentioned that it's one of the strongest in established privacy laws, so there's a lot to learn from there. It's when we hear "made-in-Alberta" practice that I'm just concerned that we're not sharing enough. That's how I see it. But I'm happy to see this collaboration. I'm happy to see the joint conversations. It's more: what can we learn from others as well? That's the spirit of this conversation.

Thank you.

The Chair: Ms McLeod, did you have a response?

Ms McLeod: Yes. I have my two points here that I will address. You know, your comments are important, and you're right; it is all hands on deck. I was at Inventures last May in many, many rooms full of very, very smart people that are doing this work, and every single one of them agreed that it needs to be regulated to ensure that we have an adequate trust model in place and that there are proper guardrails.

In terms of a global initiative, that's a nice thought. Realistically, I don't think that would ever happen. The best we could do at a global level is to define criteria that each nation-state could implement within their respective jurisdictions, but the reality is that in Canada we have a federation, so we have a Constitution that allows certain regulation at certain levels of government. You mentioned Europe. Europe, of course, is a union which is full of nation-states, so while they might be regulating at the European level, it's being implemented within the nation-states as they ratify the law and implement it in their own jurisdiction.

The GDPR is one thing, but then we also have the Artificial Intelligence Act that was just actually recently passed in Europe. They, too, are regulating separately in the artificial intelligence space. We have the AIDA legislation that's currently in draft form, and then we have different states – and I did a lot of research on this not too long ago – and they have different models, and they have different models because it depends on how they want to regulate it within their jurisdiction.

So, back to your comment about fragmentation, it is a real risk – there's no doubt about it – however, that doesn't mean that we

should stop doing what we're doing because we need to put these rules in place now before we have, you know, things happening. I mean, to a certain degree the horse is already out of the barn, and we need to try and figure out how to regulate this in a responsible way. Here our job is to protect Albertans, so that is why I made the intraprovincial recommendation for legislation in Alberta.

Quickly to scalability. The ministry talked a little bit about this earlier. It comes down to: what are you doing? If you're a small organization or if you're even a large organization and you're actually not collecting, using, and disclosing personal information or not sensitive personal information and you're not using very much of it and you're not dealing in sensitive kinds of services, your compliance obligations are going to be relatively low. However, even if you're a small business – let's say I am a retailer in a store and I'm using facial recognition technology on my clients. Well, guess what? That's going to up the ante, and you're going to have to implement rules, more security measures, and ensure that your staff understand what those rules are and build it into your infrastructure, but if you're not doing that, then, really, you don't have a lot to do. It really does depend on what an organization is doing as to how they're going to have to implement those controls in order to protect privacy. That's what we mean when we talk about scalability.

Just to comment on the nonprofits as well – and I understand where they're coming from. However, some nonprofits in Alberta process very sensitive information. We only need to look at what's happening in our health care system in Alberta. They've just stood up Recovery Alberta in the Ministry of Mental Health and Addiction. Most of the service providers in that industry are nonprofits. We have some of the most vulnerable populations, very sensitive information being processed within the nonprofit sector, and I think we owe it to Albertans to ensure that their information is protected no matter where it is being collected.

The Chair: Thank you very much.

I'll just remind everyone that we have your initial question and then one follow-up after.

Okay. Our next question comes from Member McDougall. Go ahead.

Mr. McDougall: Yes. Thank you very much, and thank you, everybody, for being here today. Ms McLeod, in your submission you explained that currently third-party service providers are not contractually obligated to comply with Alberta's PIPA legislation, which I think is a substantial risk to Albertans' personal information and privacy. Can you expand on what is the legislative gap that currently exists and why these service providers are not currently covered under PIPA?

Ms McLeod: Certainly. As it stands right now, organizations are responsible to comply with PIPA. Now, as part of the work that they do, they can actually engage service providers to assist them with various services delivery, which is quite common now. What we see often is organizations using service providers for technology-related services or other kinds of things. The service providers themselves are not subject to the legislation.

My colleagues and I are in the process of a couple of investigations that involve service providers, and these service providers actually have impacted numerous – numerous – businesses. However, we can't investigate the service provider directly – when I'm saying "we," I'm speaking from Alberta's perspective – because our legislation doesn't have that accountability mechanism built into it. What we have to do is go after the organizations. So we have a service provider that has failed to do the things that they need to do in order to adequately protect the information, yet we have to go after every organization. Now, I'm not saying that that's the wrong way to do it. However, I do think that service providers, too, need to be held accountable under the legislation for compliance with PIPA.

We see this model, for example, in the Health Information Act, where affiliates of custodians are directly accountable to comply with the legislation and I have the authority to investigate that they do so. That's the gap that we're trying to fix. This was recently addressed in the GDPR as well, so they actually have a model that not only captures service providers but also downstream service providers, and that accountability flows with them.

What I'm trying to suggest needs to happen in PIPA is that those service providers are held accountable because organizations are being held accountable where the service provider should be held accountable, and they're affecting their reputation. It's very important that we close that gap, and that's a recommendation I'd be making in all three of our laws in Alberta.

11:10

The Chair: A follow-up?

Mr. McDougall: Thank you.

As a follow-up, in your report you shared a concern for the lack of specific protections for sensitive personal information since PIPA does not set out certain categories of personal information that require additional protections or limitations such as that reveals political opinions, sexual orientation, biometric data, for example. Could you please explain: what are some of the current risks, and why should this sensitive personal information be placed under greater limitations for third-party data holders than general personal information?

Ms McLeod: I think the move towards defining sensitive categories of personal information in privacy laws actually goes to the controls and measures that strengthen the protection to protect them. Going back to my scalability comment earlier, if an organization is collecting what we now define as sensitive information, that means they have to apply more rigour to their organization to ensure that they're complying with the legislation whereas if they're collecting information that's not defined as sensitive, there are fewer controls required.

I might ask Commissioner Dufresne to comment on that as well.

Mr. Dufresne: Well, that's exactly right. That's the model that we have adopted in our guidance in terms of consent, the forms of consent, the sensitivity of information that is going to be relevant in that. The more sensitive it is, the more you're going to require it to be clear, to be expressed. In C-27 sensitivity impacts the issues of safeguards of the information and the measures that you put to protect that information. It could have an impact on retention and otherwise. It's critical, so we've recommended that those categories be defined. Right now it's defined in guidance, certainly, federally. But C-27: now the committee has adopted an amendment that would say that these are the types, some of the types. It's an open-ended list, but it includes it could be financial information, it could be health, sexual orientation, as you say. An important reminder: the law is contextual and the law is flexible and it's going to put greater onus where it needs to, and that includes sensitive information.

Mr. McDougall: Good. Thank you.

I have other questions, but I'll let my other colleagues go.

The Chair: Yeah. We'll come back to you. No problem.

Member Sweet, go ahead.

Ms Sweet: Thank you, Mr. Chair, and thank you, all of you, for being here today. I just want to go back to the education piece. When I say that, I mean how we're ensuring that citizens understand what their rights are, how they're to protect themselves. When I look at sort of how the website is set up for Alberta specifically, it's a lot of: this is the responsibility of the business; this is what they have to do under the act and legislation. I don't see a lot of education in the sense of someone like me understanding: what can I do? Like, how do I protect myself? If we go back to the conversation we were having around children and youth, how do we ensure youth understand when they're opening up those apps: what are they consenting to? What does that look like? So I'm just wondering if you have any recommendations or feedback for us as a panel around: what can we strengthen or do better to ensure that citizens understand what their protections are; like, how do they protect themselves? I appreciate we can talk about legislation about how do we hold people accountable, but part of this is also people even just understanding what those protections need to look like, I think.

Ms McLeod: Is that . . .

Ms Sweet: Yeah. Sorry. That's it.

Ms McLeod: . . . to me?

Ms Sweet: Or whoever.

Ms McLeod: Okay. Well, I'll start, and then I'm sure both of my colleagues will have comments to make on this as well. I think it's something that, you know, since the history of the office and the existence of commissioners in Alberta, however, now the growing application of these laws and the impacts – it's a very important question, and it's one that I incorporated into my business plan as ensuring that we have an engagement that includes outreach to Albertans. I created a stream in my office dedicated specifically to engagement, and I am in the process of engaging the public on the Health Information Act side of the equation. So there is some work happening in my office.

But to your point: how do we get to Albertans? I think there are a number of ways that the act actually builds that in, and that's through consent in PIPA and notice requirements. Organizations are obligated to inform people about what it is that they're doing with their personal information. I think the challenge here is that some of those policies and notifications are so complicated that nobody actually reads them. I'm sure, you know, like everyone here, I'm guilty of click, click, click so that I can get through to whatever it is I'm trying to do. So I think that some of the amendments that we're seeing, you know, notices in plain language – I talk about that in my recommendations – and ensuring that there's actual information being conveyed. I mean, if an individual on the other side of the equation doesn't care enough to read it, well, that's one thing.

But the other thing that I see in Alberta – and, you know, I'm out there talking to people all the time about privacy. I ask them about privacy. What do you know about privacy? Well, they don't know very much, so I'm going to be working hard at changing that to the degree I can, and working with children is a key part of that. You know, we want to build a culture of privacy understanding, and that starts with our kids. When I was in Yukon, I went to every school in Yukon – now, it's a smaller place – and I was so happy to be able to communicate with all the children there and talk to them about privacy, and as Commissioner Harvey mentioned, they care about their privacy. They know what that means to a certain degree, obviously, but we must do more. So I'll be working hard at trying to change that in Alberta.

I might let my colleagues talk about that a little bit as well.

Mr. Harvey: Okay. Sure. I'll start more with a general comment about privacy awareness of the society in general, and then I'll talk more specifically about children and youth. You know, I'm sure that you all have heard somebody say: oh, privacy is dead; everybody is collecting our information all over the place; there's no such thing as privacy anymore. I often reflect and imagine: what if societies had said the same thing about the environment in the early years of the Industrial Revolution when, for example, Britain's rivers were choked with pollution and its skies were choked with smog? What if they'd said, "Oh, well, you know, I guess the environment is dead, but the Industrial Revolution marches on"? They didn't. And because of that, if you're in London today or if you're in Edmonton today, we have clean air. Now, listen, this isn't to say that we wisened up and we fixed the problem because we clearly have not wisened up and fixed the problem in certain other ways, but we can learn from the successes. We're still in the early years of the information revolution, and we can learn from both the successes and the failures of the Industrial Revolution and what it did with the environment.

Privacy is not dead, is what I would say. Privacy is now just being born in that I find that in society, I often say, there's a cognitive dissonance; people are confused about their privacy. On the one hand, some people will say: oh, privacy is gone; my information is out there anyway; it's too late. But then a specific breach will affect them and they will be extremely affected by that breach. So privacy is not dead; it is just being born.

That's, I think, where it is appropriate to talk specifically about our children and youth. You reference the importance of education in that effort. It is a great pleasure to me that a number of commissioners across the country have identified children and youth as part of their strategic plans, Commissioner Dufresne and his strategic plan – I'm sure he's already referenced that, and he talked about it before – but also one of our commissioners who's not here now. Commissioner Kosseim in Ontario has identified the privacy rights of children and youth as part of her strategic plan. We around the table have signed a resolution on the privacy rights of children and youth. Nationally we've identified this as a priority, and we're advancing it.

In British Columbia, where I've just arrived, people have been asking me: what are your priorities as commissioner in British Columbia? And I say: well, I'm going to go around British Columbia and I'm going to listen to the residents of the province and what their privacy priorities are. I always lead with that, but then I always say: but I know what I'm going to hear, and I'm going to hear about the privacy rights of children and youth. It was a priority of mine as commissioner in Newfoundland and Labrador, and when I moved to British Columbia, I made it clear that it would be a personal priority of mine. The education part of that and shaping that discourse among our children and youth is a national priority and a very important one.

11:20

While there are legislative amendments, I think it's always not fair to put this on individuals themselves and say that, you know, the solution to privacy is to educate yourself. I mean, that is part of the solution, but our laws need to get their backs as well. You know, it is a national priority. We're all on it. We compare notes and learn from each other.

Mr. Dufresne: I'll just say that you're absolutely right, that we all need to do more in terms of communicating more clearly, to children in particular but to all of us. In our decision in the Facebook case that came out two weeks ago from the Federal Court of Appeal, where the Court of Appeal agreed with our findings that Facebook was breaching privacy law because they were not obtaining consent appropriately, they were not communicating the impact of going on Facebook, the Court of Appeal said that some of those privacy policies were the length of an Alice Munro short story and they were complex and people didn't read them, and even if they did, they might not understand what was going on. So there's a lot of work to be done there. We're doing it. We need to do more.

In terms of communicating with children in particular, my colleagues referenced our work with our resolution on protecting the privacy of young people. We've issued a specific version of that resolution that was addressed to parents and young people. We're trying to make our content more user friendly. I think there's more that we can do. I think our websites, or certainly my website – it's great, but it could be simpler. We're trying to do that. We're trying to use more video presentations, using all of the medium where young people are so that they can understand privacy. We're meeting with them. We're reaching out to them trying to do all of that.

In our data-scraping resolution we said many things about what organizations have to do. We also gave tips to users, what they can do to protect their information. But we always bring a caveat to that and say that, at the end of the day, we don't want to be suggesting that it's the responsibility of individuals to protect their information. They have best practices that they should follow, but organizations have to do that as well. They can't delegate this to the users. We're going to be continuing to look at that, how we can do more.

Thank you for that question in terms of concrete advice, understandable, user-friendly advice. We're going to keep focusing on that.

The Chair: A follow-up?

Ms Sweet: I'll just be really quick. It's more of a comment. I was a social worker before I was elected, and I worked with high-risk youth. This was, like – let's not talk about how long ago. It was a long time. Facebook was just becoming a thing; like, that's how long ago it was. The world has quickly shifted since then. For me when I worked in the inner city and I worked with vulnerable youth, the information that they were accessing online and who was accessing them online and all the dynamics that happened with that: it is a flag for me in the sense that because technology is rapidly changing, like, I don't even understand half of what's happening anymore because I'm just not an engaged person online. I don't particularly like it.

I do know that I've had conversations with parents around: they just don't even know what their kids are up to, right? Like, they don't understand all of the interfacing that is happening. So I think that's more to my point of: I appreciate that we have a responsibility to make sure organizations are protecting individuals' data, but with this constantly shifting environment, how do we make sure that parents understand? What does that look like, and what are sort of the key things they need to be paying attention to to ensure that their kids are being protected? I know it's bigger than PIPA. It's actually a really big conversation, but it's sort of where my head goes on a lot of these conversations.

Thank you.

The Chair: Go ahead.

Mr. Stinner: If I may make a quick addition. As should be clear by now, it is really difficult. There's no simple answer to this question, but I just wanted to draw the committee's attention to, in terms of putting things together, connecting some dots here – it was mentioned earlier about administrative monetary penalties. You know, our office made a recommendation for the committee to consider potentially putting a provision in the law that allows a judge to direct funds collected from those administrative monetary penalties towards what's known as creative sentencing, to direct those funds where they actually could make a difference to help fund initiatives that would help improve the overall compliance posture such as supporting, funding an organization that would help not-for-profits comply with privacy laws. That's something to consider here.

The Chair: Thank you.

Okay. Our next question comes from Member McDougall, if you're there.

Mr. McDougall: Yeah. Thank you very much. To Ms McLeod. As you mentioned in your submission, FOIP and HIA included the right to access one's own personal information, and while PIPA states that any individual may request their own personal information, it's not a right. Can you expand on the need to have that act clearly state that it is a right for people to own their own information and receive it?

Ms McLeod: Sure, I can expand on that. We talked a little bit earlier, I think all three of us, about moving PIPA to more of a rights-based approach as opposed to just a balancing between the collection of personal information and legitimate business uses. The purpose of that is to ensure that, you know, in this complex world of data processing, those rights are being protected at a commensurate level to whatever it is that is before us as a matter, so we can use that as an interpretation principle when we interpret the legislation.

Sorry. Just give me a second. I'm thinking as I'm responding here.

In terms of putting the right in, all it does is that it increases the ability of one to obtain access to their own information to the level of a right, and that is something that is in our Freedom of Information and Protection of Privacy Act here in Alberta. So it just recognizes the importance of that right, because having access to one's own personal information is one of the key aspects of privacy control over your information, by knowing what an organization has about you. So that's why we emphasize that need to shift it from the ability to a right.

The Chair: A follow-up?

Mr. McDougall: Thank you.

The Chair: Okay. Good.

Opposition? No. Okay.

We'll go to MLA Hunter. Member Hunter, go ahead.

Mr. Hunter: Thank you, Mr. Chair. Once again, thank you for being here.

I have a question for Commissioner Harvey. I think you were in the gallery before when we had not-for-profit organization representatives making their presentation. They say that hindsight is 20/20 vision. So you guys have already gone down this road. One of the comments that they made – and I'd like to get your opinion on this – is that they had said that by B.C. adding not-for-profits to their PIPA, it would decrease their ability to provide service. Have

you seen that happen in B.C. or if any of them have shut down because of this? I mean, it's always a balance between red tape – you know, how much can they actually do? They're voluntary. So what have you seen?

Mr. Harvey: I figured you'd ask that question, so I asked my staff: what have we seen in the not-for-profit sector? Have we seen people chafing against the administrative burden of oversight? And the answer was that we haven't; we haven't seen that; that hasn't been a factor. Instead, we provide resources to nonprofits that need and want to protect the privacy of the people that they serve. They oftentimes serve very vulnerable populations and collect very, very sensitive information, as Commissioner McLeod has mentioned, so we provide them with resources and guidelines to help keep that information safe and secure.

The answer to administrative burden is the same for nonprofits, I would say, as it is for SMEs, which is something that we've talked about repeatedly today, which is scalability and doing what's reasonable for the organization in question, having reference to the sensitivity of the data but also the capacity of the organization.

The Chair: Go ahead.

Mr. Hunter: I guess my next question is: can you give us an example, Commissioner Harvey, of infractions that not-for-profits have done that have warranted them needing to be involved in this? Now, the reason why I ask that question is because, you know, we can say, "Well, we want to protect people because we're concerned that this might happen," but were there things or examples that happened in B.C. that warranted not-for-profits being added to that?

11:30

Mr. Harvey: So I'm at a bit of a disadvantage in that regard because I'm new, so I don't have a lot of that case history at hand. I would be happy, if you wish, to provide the committee with a supplemental written submission on that question if you'd like, but I know that the small number of matters that I am aware of relate to access to personal information, so people looking for access to personal information and the not-for-profit not wanting to provide it.

Mr. Hunter: Mr. Chair, if you don't mind, I could ask Commissioner McLeod if there's been stuff coming into her office that has warranted her desire to – she wants to go down this road as well.

Ms McLeod: I'm glad you asked. I was just going to suggest that I provide a comment. I'm actually going to let my assistant commissioner Stelmack speak to this issue because she came prepared to talk about some of the things that we've been seeing over, you know, the history of PIPA in the office as it relates to nonprofits.

Ms Stelmack: Yes. Thank you. Yes. We have seen, for example, access requests from people who work for nonprofits as employees and they want access to their employee files and weren't able to get access to those because it's not under PIPA. I've also seen some confusion in terms of that layer of "What is a commercial activity?" outside in the public and, as well, in our office in interpreting that. It's very difficult. We often turn ourselves inside out as to whether or not the nonprofit is a commercial activity.

A good example is that there was a privacy breach in 2020 of something called Blackbaud. It was a service provider to many charities and nonprofits across North America, and the organizations would report to our office about breach reporting. These were things like donors lists, sometimes, you know, what people's interaction with these charities were, and there was a lot of confusion as to whether or not the organizations were required to report to notify affected individuals on whether or not what was breached was involved or collected or used and disclosed in the course of a commercial activity. These breaches affected thousands of Albertans, and there was a lot of confusion in that area.

Even sports associations quite often come to us and say: "You know, we're selling jerseys. Is this a commercial activity?" Or hockey clubs: "We charge fees to enter the hockey club. Do we need to protect the personal information of the children commensurate?" So I would say that it does cause confusion when there's not one law for all, and it does require a lot more thinking around whether what you're doing is clearly a commercial activity or not, and sometimes those lines are not very clear.

The Chair: Member Dyck.

Mr. Dyck: Excellent. Thank you, Chair. I guess I just have potentially a question for all of you. We've talked a little bit about social media, and then I guess my question comes in: what is your view on personal responsibility on privacy issues? For me, on social media most people want their information to not be private. In many ways they want their information, maybe an article or something, their posts, to be public. When I'm talking to youth and particularly under 18, they want to be social media influencers; they want to be YouTube stars. Their goal is that they share their information with the world, so how do we coincide those desires of a youth particularly – I'm not talking about an adult right now but a youth specifically – and their desire to share publicly while also keeping their information private?

This is particularly – I guess I would ask a second follow-up in that when there's opportunity for companies to see that data publicly, then all of a sudden that child's goal is being accomplished. So how do we balance that? Maybe a different question is: how do we offer both of those extremes at the same time? I would love your thoughts on that. I do have a follow-up question as well.

Ms McLeod: Okay. I'll start, and then I'm sure both my colleagues have something to say. So privacy is about control of one's own personal information. I choose which organization I want to share my information with, and that organization is bound by rules to ensure that that information is being used for the specific purpose that I'm actually putting it out there. So if I make my information accessible via a social media app, that means that organization is obligated to protect it in accordance with what it is I'm doing. That doesn't mean that that organization then gets to go sell my data or gets to do anything else that they want to with my data, because there's a specific engagement that I'm having with my own personal information and a particular organization. That's what privacy law is about. It's about control.

In privacy laws there's also the ability to use publicly available information in certain circumstances. "Publicly available" is a defined term, and essentially what it means is things like registries, that are accessible to the public, and then you can use that information as a member of the public. Because information is accessible on a social media website does not make it publicly available.

Here's where the confusion lies, that we have some organizations out there right now, Clearview AI being one of them, that we are now in court about, that scraped the data off websites and social media sites in order to create a business model. You're not allowed to do that. That's where the privacy laws come into play. I control my information, these organizations are obligated to follow those

rules, and it's not a free-for-all for everybody, despite what people may think. So I think that there's some confusion in there. We see that in business models that are scraping the Internet of information when the privacy laws don't allow them to do that.

That's my comment, and my colleagues might have more.

Mr. Dufresne: Well, just briefly, I think your question touches on the issues of consent, the issues of purpose, right? In terms of consent, well, questions have been raised by ourselves, by courts, by commentators about: do people truly understand and consent to what's going on? They may think that it's being used only by their friends, close knit. They may be very comfortable with that. They may be very comfortable with one company. But we know, as recently as into our Facebook case, concerns about how really, truly understandable those long privacy clauses are.

The role of opt-in, opt-out recently with LinkedIn – there was an automatic opt-in to train AI models. I didn't know that. I'm a LinkedIn user; I didn't know that. I found that out. So we reach out on that. The international community is reacting, and now they've turned it off. So there are questions on that.

There are questions with AI. We can do more and more with information. Do people truly know what they can do with just a little fragment of my voice? They can do a deepfake and then use that to defame me or to influence political campaigns and so on.

I think there are lots of questions about consent that privacy law is dealing with. And then purposes: if you consent to it for certain purposes, even for public purposes, are you consenting to an organization like Clearview AI creating a police lineup with your face forever and selling it to law enforcement around the world? No, you're not. Are you even consenting it to being used to train models? I think those are the questions. I understand that it may feel like, well, people are good with that because it's public, but there are these questions that arise.

Mr. Harvey: I think I might just try to add some additional colour. Really, where Commissioner McLeod started by saying that we've got to start with privacy equals control: I think that's the most important principle. I'm just going to add a couple stories that will add just a little bit of colour to some of this. I really love this topic.

The first one is that a couple of years ago I went to a conference and one of the keynote speakers was a sociologist. Actually, I believe she was a criminologist. I don't know how she came to research this particular topic as a criminologist. Nevertheless, it was a really interesting lecture. What she was studying was precisely the question that I think you're getting at, which is: what are the attitudes of children and youth? We see them act online. What are their attitudes about their privacy online? And what she found was that our children, our youth in particular, were very, very clever about how they curated – and this is a term that you use. I used this term, again, in my opening remarks as well briefly, but I love to have the opportunity to delve into it a little bit more.

Our children and youth can be very clever about how they curate their online personas. Many of them have multiple accounts, each with different permission settings, depending on who they want to access what, okay? She told the story of this one girl in particular. She was interviewing these youth, and this one girl in particular: you know, she looked at her Instagram account, and then she went and met with her. The Instagram account had all these pictures of horses, so she sat down with this girl and she said, "Oh, I see you're interested in horses," and the girl was like, "No." She said, "But your Instagram account is all horses," and she said, "Well, I thought that was, like, something cool and niche, so I wanted to have, you know, a horse girl persona," a totally fictionally created horse girl persona. Her real identity, the different layers of her identity – she had a real identity. That was locked down to a very small circle of friends. This speaks to control.

11:40

Okay. I'll tell another story. I should mention at the outset that I'm going to talk about my experience as a parent. My daughter is okay. I've asked her: am I okay to talk about this in public? She's okay with it. My daughter has multiple different accounts, as daughters do and sons, too. One of these accounts, we found out – my son knew about this, but neither of my wife and I did. She had a TikTok account. You know, I feel professionally obliged to be dubious about this. She had had this secret TikTok account with something like 10,000 to 20,000 followers, and she kept it secret. The only person in her real life who knew about this TikTok account was her brother, my son. None of her best friends knew about it. It involved reviewing anime. She was afraid that if people found out that she was into anime, then she might get made fun of for that, so she didn't tell even her best friends about this and then eventually closed it down.

What's important here is that what our kids intuitively want and try to be very clever about is not just throwing their information out there for it to be discovered – sometimes that's indeed what they want – but doing it in a very controlled and curated way.

There are two points here that I think are important because of what it means for us, for you as legislators and for us as regulators. We need to give them the control that they think that they have because – and this is the second point – our youth are very clever, but they're nowhere near as clever as they think they are. They may think that they are very cleverly protecting all their information, but many youth were not protecting their images from the facial recognition scraping that was being conducted by Clearview AI. It is, I think, our responsibility as regulators – and I think legislators have a responsibility to give our youth but all of us the controls that we deserve so that we can thrive in an online environment and live the lives that the people that you've talked to want to live.

Mr. Dyck: Can I have a follow-up, Chair?

The Chair: Yeah. Go ahead.

Mr. Dyck: Okay. Going in a different direction, I just want clarity. Commissioner Harvey – and I apologize if I missed it – you were talking about deception by design, I believe, on some apps. Can you expand on that? I understand that there are bad marketing practices and there are good marketing practices. Deceptive by design: I want to understand what those are. Can you just give me a little bit of a fuller scope of what that looks like?

Mr. Harvey: Sure. Actually, MLA Sweet was talking about the importance of kind of communicating and educating earlier. After we did our sweep – all three of our offices were involved in the sweep, the global sweep, that we did. As a result of that, we did this infographic that we put online. Actually, if you're interested, you might want to go to the oipc.bc.ca website, where we have an infographic that captures a list of these. It's really interesting because you look at them and some of them are so ubiquitous in website design that we find – I think the number of, like, almost all websites that we find have some of these, and some of them are as simple as opt-in, as Commissioner Dufresne was referencing. Using opt-out rather than opt-in is on one spectrum of that deceptive design spectrum.

On the other are what we call the dark patterns that will use emotional tools from behavioural psychology to try to manipulate you into feeling bad about doing a thing such as, for example, when you get a text prompt that says – oh, you know, let's say we're

talking about Duolingo here. Duolingo: the language app that we all – you know, not we all but many people – use to try to brush up, let's say, for example, my rusty French. When I stop using it, I get a text prompt that says: oh, Duo is really sad that – you know, Duo misses you and wants you to come back and do your French lesson. Okay. Well, there are really insidious examples of these in, particularly, apps that target children that will try to make them feel guilty for not providing more information. They may use tools like saying: well, everybody else has this option turned on; you should, too.

These kind of tools of behavioural psychology are being used, and really my worry is that they become so ubiquitous that they are now normalized. People have said: well, you know, that's just clever marketing. These things, these tools: we are of the view – and not just not just us, but there's a global consensus among privacy regulators that this is beyond good marketing, that these are deceptive and manipulative tactics to try to squeeze people into providing more information about themselves so that they can then use this information to then further manipulate them. This isn't good marketing; this is deceptive marketing. That's not what we want.

The Chair: Okay. Thank you very much.

We'll go to Member Sinclair.

Mr. Sinclair: Thank you, Mr. Chair. Thank you, Commissioner Harvey. This is another question for you. I just wanted to mention earlier: I appreciate the land acknowledgement. It's very classy.

In your submission you encourage the committee to consider specific protection for children's personal information. Could you provide some examples on what type of protections could be included in this act for this purpose? I know you mentioned the acronym there, AMPs, I think, the administrative monetary penalties. I'm not sure if that's – if you could expand maybe if it falls in there.

I appreciate your candid comments here, because I think that it, for me, is normalizing the behaviour for most people in the last 15 years with smart phones, and I'm sure most people in this room are guilty of it. It's quickly on to the next thing, so you're quickly scrolling a bunch of agreements just to click off "agree," and our kids are also watching and parroting this behaviour.

I'm also a believer, though, in the personal responsibility of the parent to be able to monitor my children's activities, like the way you explained you are, but I think there's an important balance here where you guys have to come in and be able to be the guardians for us, especially – I consider myself a young boomer when it comes to technology, but being able to manage the dangers that we can't see as parents and put in safeguards that are common sense, that make sense, like opt-out instead of opt-in, something as simple as that, where it's just not so accessible for children to be able to give away their private information. If you could include a specific on B.C.'s protections for children's information in their recent changes to privacy legislation.

Thank you.

Mr. Harvey: Thanks. I'll start by saying that B.C., you know: we've made recommendations. My office did. That's prior to my arrival. We made recommendations to B.C. to amend its PIPA some time ago, but that act has not yet been reformed. We remain optimistic that it has. The government of the day, who – as the commissioner referenced, I can't speak for the government of British Columbia. As an officer of the Legislature I can't speak for British Columbia, but I know that the British Columbian government did table although did not advance an online harms bill and has been talking to tech companies about these kind of things.

So what kind of things specifically are we talking about? We're still working through this in the OIPC about what we're recommending. We have talked about things like a children's code. In the U.K. there is a children's code introduced by the Information Commissioner's office. Under that regime the commissioner has code-making power that is essentially like regulation-making power. In the OIPC we think this is an interesting possibility although I'm not sure that that's the first thing that we'd go to. That's not really – we're not promoting, at this juncture, something exactly like what's in the U.K. that establishes a children's code. But you could also look in California, where there's also a children's code, and the children's code in California is actually an act of their state Legislature, so it's a law.

11:50

So what are we talking about in B.C. that can improve things for children? That's where I came to the AMPs – that is, administrative monetary penalties – and saying that the most important thing we can do at this juncture is really strengthen our enforcement powers across the board for children and youth but also for everybody else just so that we can get tech companies, when engaging with us, to essentially take us more seriously. The idea of AMPs: you know, as I said in my submission, their value is not so much in levying them but in having them available to bring people to the table. That's, I think, the reason why I focused on AMPs.

But the last thing I'll make, and then I'll hand things over, is to talk about, you know, what would be some of the specific tools. Here I just want to reiterate something that both of my colleagues have mentioned, and that is the importance of plain language and the fact that our children and youth do not have the ability to really understand their privacy policies. How can they control their information if they can't understand what's being collected and used about them? Plain language, and plain language that is done in a way – so this is where we get to the children and youth specific part of it – that companies need to understand who their audience is, and their plain language needs to be plain to their users, so a site whose users are children needs to have a certain type of plain language. Plain language for youth needs to be different. I hope that answers your question.

Mr. Sinclair: Thank you. That's good.

The Chair: We've got two more sets of questions on the government side, and then we'll wrap it up.

Member Armstrong-Homeniuk, go ahead.

Ms Armstrong-Homeniuk: Thank you, Chair, through you to the B.C. commissioner. I want to talk about the recommendations by the Information and Privacy Commissioner of B.C. – obviously, yourself – in regard to automated decisions to allow individuals to request the reason why a certain decision was made by an automated system and object to the decision, which should be then brought before a member of the organization with the authority to review or reverse a decision. Could the office of the Information and Privacy Commissioner of B.C. expand on the importance to contest automated decision-making, and would something like this apply only to AI systems?

Mr. Harvey: Thank you for that question. Even though the heading here and the heading in my written submission – and it mirrors our submission that we made to our stat review committee back in 2021, I believe. At the time, it said "automated decision-making," but if you look at the footnote here, there's a reference to algorithmic decision-making. I think that's probably the better term.

If we were going to move forward, if B.C. was going to move forward on this, we would ask them to very carefully look at what's going on with C-27 and AIDA, the Artificial Intelligence and Data Act, that are before the federal Parliament to assure alignment, ensure we don't fall out of harmonization. But the answer to your question: what will we be looking for? It really is to try to align the needed regulation of AI systems with the basic privacy principles that privacy legislation across the country is based on. The important principles here are transparency and accountability. We believe that people have a right to know if a decision that is being made about them is being made by AI, so they have that transparency, and that there is an ability to appeal that and that there's an accountability for that. These are all kind of part of the 10 privacy principles that inform all of our legislation. In that specific recommendation what we were doing is that we're saying: this is how they should apply to the AI context.

But in your question I detected a concern. Are we talking about every automated processing? You know, a lot of processing is not algorithmic; it's just straight kind of screening. I think that there are often privacy issues with screening that are not informed by algorithmic decision-making. But the problems with it aren't quite so acute and requiring a specific framework as is the algorithmic decision-making, so I really bear down on that phraseology.

Ms Armstrong-Homeniuk: Thank you.

The Chair: Okay. Our last question that I have right now is Member Dyck. Go ahead.

Mr. Dyck: Well, thank you very much. This is specifically for Commissioner Harvey again. I just want to talk about or get your thoughts on provincial parties' privacy practices. You guys are the only jurisdiction, I believe, in Canada that has it. We've received different feedback on this. Can you just expand what these changes specifically are, and what has this meant for your office and the citizens of B.C.?

Mr. Harvey: As I mentioned in my opening submission, political parties are treated in British Columbia just as any other organization because the act does not differentiate among organizations. A political party would be treated the same as an SME or an amateur sports organization. As I said in my opening submission, what we have found is that it has worked quite well. That's not to say that there haven't been concerns, but those concerns were brought to light. I direct you to – and my written submission, I think, makes reference to this – the 2019 investigation that my predecessor did into political parties in B.C. at that time, and that brought forward a whole range of recommendations about how political parties at that time were collecting, using, and disclosing personal information and recommendations about how they would improve that protection. That report led to, as I said, a series of recommendations, and in our view it has led to significant improvements to the benefit of people in British Columbia.

Just to illustrate what that looks like in today's language – and I'm going to speak at a bit of a high level because this is an ongoing and fluid situation. I'm sure that as our neighbours you've noticed that there was recently a change in the political landscape in British Columbia whereby the B.C. United decided that they – even characterizing the decision about what they decided to do is a little tricky. But I guess what they've decided to do is that they were not going to run any candidates and withdrew the B.C. United nominations of all of their B.C. United candidates. Then some of those candidates are now running as B.C. Conservative candidates, and some of them are running as independents. Questions were raised about: what happens to the information that was collected by all of those B.C. United candidates? What are they able to do with it and not do with it? Now there are some B.C. Conservative candidates who are no longer running as B.C. Conservative candidates but who are running as independents. What about the information that they have?

Without going into detail, what I can say is that people had questions about all of that. Some people: let's say that they had their B.C. United candidate knocking at their door and collecting information about them. Some of it may be sensitive information to them such as voting intention that they may have given to a B.C. United candidate. They may not want that information to be given to the B.C. Conservative Party, right?

The benefit here is that we're on it, okay? As the B.C. OIPC we're on it. We're in communication with the parties. We're talking to them about it. You know, discussions are being had. There is oversight is the answer to the question. The reality is that there is someone looking at that. If we were in a jurisdiction where there was no provision about this in PIPA, then I wouldn't be able, I wouldn't have the authority to write to the parties and say: what are you doing? You know, I wouldn't have the mandate to say: let's have a conversation about your privacy policies. But we are in that situation, and I think that British Columbians are the better for it.

Mr. Dyck: Thank you.

The Chair: Thank you very much.

Just the last call for questions. No? Okay.

That concludes the oral presentations we will hear today. I would like to thank the three privacy commissioners and all other guests for presenting to us and responding to our questions. They were really good questions and really good answers, and this was a really good event today. Again I'd like to thank Commissioner Harvey and Commissioner Dufresne for travelling and taking extra time out of your schedules to meet with us in person.

12:00

There were some committee requests for a written response, so if we could get those within 30 days, that would be appreciated. Okay. Great. You're allowed to leave, and thank you for coming.

We have a couple other items of business to deal with. Our next step. Hon. members, are there any other matters that the committee members have questions about or wish to speak to in relation to the information-gathering phase of the Personal Information Protection Act?

If not, we will now move to the next phase of our review, deliberations and making recommendations for our report back to the Legislative Assembly. The standard process at this time would be to direct the Legislative Assembly Office research services to prepare an issues and proposals document summarizing the recommendations contained in the written submissions and oral presentations provided to the committee. At this time I would like to open the floor to any comments, questions, or motions regarding this matter.

Mr. Dyck: I would just love to move that motion to do so with the LAO, unless there are other comments prior.

The Chair: If you want to go ahead and read that.

Mr. Dyck: You bet. Thank you, Chair. I move that

> the Standing Committee on Resource Stewardship direct the Legislative Assembly Office to prepare a summary of the issues and proposals identified in written submissions and oral presentations made to the committee in relation to its review of the Personal Information Protection Act.

The Chair: Okay. Any discussion?

All in favour, say aye. Any opposed? Online, if you're in favour, say aye. Okay. Opposed?

That is carried.

Are there any other issues for discussion in today's meeting?

The date of the next meeting will be at the call of the chair. If there's nothing else for the committee's consideration, I will call for a motion to adjourn. Mr. Eggen. Any opposed? Carried.

Thank you very much, everybody. That was great.

[The committee adjourned at 12:02 p.m.]

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