



Legislative Assembly of Alberta

The 31st Legislature  
First Session

Standing Committee  
on  
Resource Stewardship

Personal Information Protection Act Review

Thursday, April 25, 2024  
9 a.m.

Transcript No. 31-1-11

**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)  
Bouchard, Eric, Calgary-Lougheed (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)  
van Dijken, Glenn, Athabasca-Barrhead-Westlock (UC)\*\*

\* substitution for Scott Sinclair

\*\* substitution for Nolan Dyck

**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
Teri Cherkewich	Law Clerk
Trafton Koenig	Senior Parliamentary Counsel
Vani Govindarajan	Parliamentary Counsel
Philip Massolin	Clerk Assistant and Director of House Services
Nancy Robert	Clerk of <i>Journals</i> and Committees
Abdul Bhurgri	Research Officer
Christina Williamson	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
Shannon Parke	Communications Consultant
Janet Schweigel	Director of Parliamentary Programs
Amanda LeBlanc	Deputy Editor of <i>Alberta Hansard</i>

## **Standing Committee on Resource Stewardship**

### **Participants**

Ministry of Technology and Innovation

Hilary Faulkner, Executive Director, Privacy, Policy and Governance

Meredith Giel, Director, Access Policy and Privacy



9 a.m.

Thursday, April 25, 2024

[Mr. Rowsell in the chair]

**The Chair:** 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 Rowsell, 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, and we'll begin to our right.

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

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

**Mr. van Dijken:** Glenn van Dijken, Athabasca-Barrhead-Westlock.

**Mr. McDougall:** Myles McDougall, Calgary-Fish Creek.

**Mr. Bouchard:** Eric Bouchard, Calgary-Lougheed.

**Mr. Stinner:** Chris Stinner, Assistant Commissioner, strategic initiatives and information management.

**Ms Stelmack:** Cara-Lynn Stelmack, Assistant Commissioner, case management, OIPC. Thank you.

**Ms McLeod:** Diane McLeod, Information and Privacy Commissioner.

**Ms Faulkner:** Hilary Faulkner, executive director of privacy, policy, and governance with Alberta Technology and Innovation.

**Ms Giel:** Meredith Giel, director of access policy and privacy with 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 Steenbergen:** Good morning. Christina Steenbergen with LAO communications.

**Dr. Williamson:** Morning. Christina Williamson, research officer for LAO.

**Ms Govindarajan:** Vani Govindarajan, Parliamentary Counsel.

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

**Mr. Huffman:** Warren Huffman, committee clerk.

**The Chair:** Okay. For the record I'd like to note the following substitutions: Member van Dijken for Member Dyck and Member Bouchard for Member Sinclair.

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 transcript of the meeting can be accessed via the Legislative Assembly website. And there's no one online and no one on the phones.

**Mr. Huffman:** Actually, I think maybe Member Al-Guneid might be there.

**The Chair:** Okay. We have Member Al-Guneid, I think, online. If you could introduce yourself.

**Mr. Huffman:** I'll try to work it out with her.

**The Chair:** All right. Perfect.

Okay. We'll go to the approval of the agenda. Are there any changes or additions to the draft agenda? Go ahead.

**Mr. Schmidt:** Thank you, Mr. Chair. I have a motion to move on the agenda. If I could have that brought up onto the screen, please. Thank you. I move that

the Standing Committee on Resource Stewardship amend the proposed agenda for its April 25, 2024, meeting by moving request for inquiry to item 4 and review of the Personal Information Protection Act to item 5.

**The Chair:** Okay. Any discussion? Go ahead, MLA Hunter.

**Mr. Schmidt:** Mr. Chair, if I could provide some justification for the motion.

**The Chair:** Okay. Go ahead.

**Mr. Schmidt:** Thank you very much. We have an e-mail from – let me just see – Deborah Dean in Calgary, Alberta, who wrote to the chair of the Standing Committee on Resource Stewardship and to all members of the Standing Committee on Resource Stewardship requesting public input to Bill 2, the Alberta Pension Protection Act. The reason that I'm bringing forward this motion to move this item up on the agenda is that I believe – well, two things.

We have a rather lengthy agenda, Mr. Chair. I am afraid that, given the other things that are on the agenda, we might not get to this item today, and that's one of the reasons that I'm proposing that we move it up, so that we actually address this item and not run out of time and end up deferring this item to some other time when the committee has to meet. I note that there are no scheduled meetings for the committee right now, so we don't know, if this item is deferred, when the committee will get to it.

Second of all, Mr. Chair, I do believe that this item is of significant importance to the people of Alberta. I know that I've heard from many of my constituents in Edmonton-Gold Bar that they are deeply frustrated with this government's refusal to listen to the people of Alberta and have their opinions heard on the Alberta Pension Protection Act. We've seen multiple occasions that this government has refused to listen to the input of people and to have their opinions heard on this. We know that the Premier has refused to have in-person meetings with Albertans, instead choosing to have scripted town hall meetings over the telephone. We know that every time we've pressed the government in question period to hold in-person meetings, they've refused to do so. They won't release the results of the online survey that they've produced. So the people of Alberta are rightly frustrated that the government refuses to hear their voices. I think that by adopting this motion and dealing with this item first, the committee can show the people of Alberta that their opinions on the Alberta Pension Protection Act are something that are important and that are deserving of the attention that the people are asking them.

So for those reasons, Mr. Chair, I am bringing forward this motion to deal with this item first. Thank you.

**The Chair:** Okay. Any other discussion? Go ahead, MLA Hunter.

**Mr. Hunter:** Well, Mr. Chair, as the hon. member has pontificated most eloquently, I would have to say that I disagree. The committee is currently undergoing a review of the Personal Information Protection Act, and the ministry officials and officer are currently waiting to provide presentations. This is important work that we've undertaken, and I think that it's important for us to be able to get to that, and we can do other business, as is typical, at the end.

**The Chair:** Okay. Thank you very much.  
Okay.

**Mr. Schmidt:** Yeah. Well, thank you, Mr. Chair. You know, just in response to Member Hunter's statements, I do appreciate the time that the civil service and the office of the Information and Privacy Commissioner have made to attend this meeting. I don't think that dealing with this item before we get to item 4 – or it would be 5 – on the agenda would necessarily mean that their time is not well spent. We will absolutely have time to get to them. It's just that we need to make a decision, I think, on item 5 before we deal with the protection of information and privacy act.

**The Chair:** Okay. Go ahead. One more. MLA Hunter.

**Mr. Hunter:** Yeah. I think that's right. We need to get on to make a decision here, so let's vote.

**The Chair:** Yeah. Okay.  
Member Al-Guneid, if you can introduce yourself, please.

**Ms Al-Guneid:** Hi, everyone. Nagwan Al-Guneid, the MLA for Calgary-Glenmore.

**The Chair:** Are we done? Okay. We're wasting a lot of time here.

**Mr. Eggen:** Yeah. We're going to vote now, right? Can we record the vote, please?

**The Chair:** Yeah, we could.

**Mr. Eggen:** Thank you.

**The Chair:** We've got to do a voice vote first.  
Okay. On the amendment, all those in favour, say aye. Online? Okay. All those opposed, say no. All right.  
That is defeated.

We'll go to the recorded vote. A recorded vote has been requested. The process for a recorded voting in committee is similar to the process for a division in the House. I will first ask those in the room who are in favour of the motion to raise their hands, and the committee clerk will call the names of those who have raised their hands and record the vote. We will then follow the same process and go to against the motion. Those in favour would raise their hands.

**Mr. Huffman:** We have hon. Member Schmidt and hon. Member Eggen in the room.

**The Chair:** So we just can't do the online one? Is that the way it is? Everything in the room first. Okay.  
Those opposed to the motion, raise your hands.

**Mr. Huffman:** We have hon. Member Armstrong-Homeniuk, hon. Member Hunter, Member van Dijken, and Member McDougall.

**The Chair:** And Member Bouchard.

**Mr. Huffman:** And Member Bouchard. I'm sorry.

**The Chair:** Okay. Online, if you can hear us, cast your vote. Go ahead. That's a shame. Okay.

Member Al-Guneid, online, can you hear us? If you could cast your vote.

**Ms Al-Guneid:** Yeah. I'm voting in support of the motion.

**The Chair:** Okay. Very good. Thank you.

9:10

**Mr. Huffman:** Thank you, Mr. Chair. For the motion, three; against, five.

**The Chair:** Okay. Very good.  
That motion is defeated.  
We'll now go for a motion to approve the agenda.

**Mr. Hunter:** Mr. Chair, I move that the Standing Committee on Resource Stewardship approve the proposed agenda as distributed.

**The Chair:** Okay. Thank you.  
All in favour? All opposed? Okay. That's carried.  
Okay. Minutes. Next we have draft minutes of our January 22, 2024, meeting. Are there any errors or omissions?

If not, would a member like to make a motion to approve the minutes?

**Mr. Hunter:** So moved.

**The Chair:** Thank you.  
All in favour? Any opposed? Thank you. Carried.  
Okay. We're here to review the Personal Information Protection Act. We have some technical briefings. Hon. members, at our last meeting the committee invited the Ministry of Technology and Innovation and the office of the Information and Privacy Commissioner to provide technical briefings on the Personal Information Protection Act. I would like to invite them both to provide their briefings, and we will have a joint question-and-answer period after.

To begin, I would like to turn the floor to Maureen Towle, Hilary Faulkner, and Meredith Giel from the Ministry of Technology and Innovation. You'll have up to 20 minutes for your technical briefing. Before you begin, please introduce yourselves for the record.

**Mr. Huffman:** They've already done that.

**The Chair:** Okay. You don't have to worry about that. Your time will start when you begin your presentation.

**Ms Faulkner:** Good morning, Chair, members of the committee, and others present. My name is Hilary Faulkner. As I said, I am the executive director of privacy, policy, and governance with Alberta Technology and Innovation. Thank you very much for the opportunity to speak with you today about the Personal Information Protection Act, or PIPA. Before I speak to some of the act specifics, I do want to provide some information regarding where PIPA services reside in the government of Alberta.

Technology and Innovation is the ministry responsible for PIPA. The privacy, policy, and governance branch in Technology and Innovation performs several functions, including leading the enhancement and development of policy instruments related to content management, which includes data information and records management as well as privacy, including FOIP and PIPA. In addition, the branch provides training and compliance activities across the government of Alberta in support of this legislation and

policies. The branch also manages the government of Alberta's FOIP/PIPA help desk, which provides general guidance about FOIP and PIPA to Albertans. The accountability to uphold the intent and rights within FOIP and PIPA is shared with the office of the Information and Privacy Commissioner.

Moving on to slide 2, I will now speak very broadly to what privacy is before getting into PIPA specifics. Privacy is not defined within PIPA or within any other privacy legislation in Canada. However, broadly speaking, privacy is the right to be let alone or freedom from interference or intrusion. The foundation for the right to privacy stems from the Canadian Charter of Rights and Freedoms, which does not specifically mention privacy or the protection of personal information. However, it does afford protection under section 7, "the right to life, liberty and security of the person," and in section 8, "the right to be secure against unreasonable search or seizure." Information privacy is the right to have some control over how your personal information is collected and used.

In today's digital age Canadian consumers and citizens increasingly recognize the benefits of sharing their data with businesses and expect organizations to use consumer data to deliver the products and services they want and need. As greater amounts of information are managed by governments and private-sector organizations, public concerns around the collection and use of personal information have correspondingly increased, particularly as the result of information being exploited or mishandled. In order to reflect the changing realities of the digital economy, modernization of privacy laws needs to find the balance between providing effective privacy protection for Albertans and enabling Albertans to enjoy the social and economic benefits of data use.

Moving on to slide 3, there are currently a number of access and privacy laws that apply in Alberta, PIPA being one. The Freedom of Information and Protection of Privacy Act, or FOIP, applies to public bodies, which includes organizations like the government departments, schools, provincial police, and municipalities. FOIP is authority based, which means the act itself places limits on the collection, use, and disclosure of personal information. The Health Information Act governs and protects health information in the custody or control of a custodian. Examples of custodians are the Ministry of Health, pharmacies and pharmacists, optometrists, registered nurses, and dentists.

The Personal Information Protection and Electronic Documents Act, PIPEDA, is the federal version of PIPA. PIPEDA applies to federal works, undertakings, and businesses. Organizations subject to substantially similar provincial privacy law are generally exempt from PIPEDA. However, PIPEDA does apply to provincial organizations when they engage in commercial activities across Canada. Common examples of federally regulated businesses include telecommunications companies, airlines, and banks. Our focus today, though, is the Personal Information Protection Act, or PIPA.

Moving on to slide 4, PIPA has been deemed substantially similar to PIPEDA. As I mentioned previously, this means that organizations subject to PIPA are generally exempt from PIPEDA with respect to the collection, use, or disclosure of personal information that occurs within the province.

PIPA is a consent-based legislation, meaning that it primarily relies on consent for the collection, use, and disclosure of individuals' personal information by individuals and organizations operating in the private sector. There are only limited and specific circumstances set out in PIPA when consent may not be required. Consent can include express consent, implied consent, and consent by not opting out.

Express consent is when consent is provided in writing or verbally. For example, when a customer signs up for a loyalty program at a grocery store and the customer signs a consent form explaining the use and disclosures of their personal information, they are giving express consent.

Implied consent is when an individual does not actually give consent but volunteers information for an obvious purpose and a reasonable person would think that it is appropriate in this situation to volunteer that information. For example, when an individual takes a shirt to a dry cleaner, the employee asks for their name and phone number, and the individual provides these voluntarily. Consent is implied that the dry cleaner can use their name and phone number to identify the individual when they come back to collect their shirt or contact them if they forget to pick up their dry cleaning.

Finally, opt-out consent is when an individual is given the choice to opt out of collection, use, or disclosure of their personal information. By not opting out, they have provided consent to the organization. For example, an individual enters a draw to win a prize and provides their name and home e-mail address. The draw form clearly provides space to check off if they do not want to receive more information about similar products from the company, providing the individual the opportunity to opt out of their information being used for that purpose.

PIPA aims to balance the obligation to protect personal information with the private sector's need to collect, use, access, and disclose personal information to provide goods and services. With the shift towards an increasingly digital world and new challenges to privacy, it is important to explore potential modernization of privacy protections to ensure that this balance is maintained.

The purpose of PIPA is to govern the collection, use, and disclosure of personal information by organizations in a manner that recognizes both the right of the individual to have their information protected and the need of the organizations to use that information for reasonable purposes. PIPA provides individuals with the right to request access to their own personal information while providing a framework for conducting the collection, use, and disclosure of personal information for reasonable purposes appropriate for the circumstance.

Some key elements of PIPA to highlight include that organizations that are subject to PIPA must develop and follow policies that are reasonable to meet the organization's obligations under the act. Organizations must designate one or more individuals to be responsible for ensuring the organization complies with PIPA. This designation is commonly known as a privacy officer.

Notification, with the exception of implied consent, is required before or at the time of collecting personal information. Notification is also required when an organization uses a service provider outside of Canada to collect personal information for or on behalf of the organization. There are special rules in PIPA for the collection, use, and disclosure of personal employee information and on business transactions, specifically in relation to disclosure respecting acquisition of businesses.

Finally, notification of loss or unauthorized access or disclosure, so breach reporting, is a requirement in PIPA, and an organization must notify the Information and Privacy Commissioner and potentially impacted individuals if there exists a real risk of significant harm.

#### 9:20

PIPA includes a standard as to what is reasonable, which is also referred to as a reasonable person test, for an organization to justify why it is collecting, using, or disclosing personal information. An

example of a reasonable person test would be if an individual is asked to fill out a tenant application form and on the form the landlord asks for the applicant's social insurance number and bank account so that the landlord can cross-check information on the applicant's credit report. While the landlord needs to screen prospective tenants, requiring this type of personal information is not reasonable for this purpose. A less privacy-invasive way would be determining the applicant's reliability by obtaining references from former landlords.

Moving on to slide 5, a brief history of the evolution of PIPA, the act was passed on December 3, 2003, and has been subject to a number of amendments since it was first proclaimed, in 2004. It was amended in 2005 to align with the Health Information Act, the Election Finances and Contributions Disclosure Act, and the Post-secondary Learning Act as well as addressing key concerns relating to legislative review and OIPC jurisdiction.

On May 16, 2006, the Legislative Assembly of Alberta appointed an all-party select special committee to review PIPA. The committee submitted its final report on November 14, 2007. In response to this report, the government of Alberta introduced Bill 54, which passed on October 27, 2009. The 2009 amendments added special provisions for transparency when using service providers outside of Canada and mandatory breach notification provisions.

Further, in 2014, in response to a Supreme Court decision, PIPA was introduced in the Legislature on November 18, 2014, and received royal assent on December 17, 2014. This amended PIPA to allow trade unions to collect, use, and disclose personal information without consent to inform or persuade about a matter of significant public interest or importance about a labour relations dispute.

The act was again reviewed in 2015 by the Standing Committee on Alberta's Economic Future. However, no amendments were implemented as part of that review. The last special committee review began on September 27, 2022. However, this review was not completed as the dissolution of the Legislature occurred as a result of the May 2023 election, stopping the review.

Moving on to slide 6, this slide provides an idea of those organizations to which PIPA is subject and those to which it does not apply. On the left-hand side of the slide the list includes organizations that are subject to PIPA. This includes corporations, trade unions, and partnerships. It is important to note that nonprofit organizations can also be subject to PIPA but only to the extent that those organizations are involved in a commercial activity. A commercial activity means a transaction, act, or conduct that has a commercial character to it such as the selling, bartering, or leasing of donor, membership, or other fundraising lists. It also includes operating a private school or college or an early childhood services program.

The right-hand portion of the slide provides a list of organizations that are not subject to PIPA. This includes individuals acting in a personal way relating to their home and family, organizations that are subject to the FOIP Act, and political parties, who are also not subject to PIPA.

Moving on to slide 7, the digital age is fundamentally transforming society. Data of all kinds is being collected at unprecedented rates and used to inform everything from consumer habits to government and business services. Rapid technology shifts are fostering academic advancement, offering innovative solutions to age-old problems, driving economic growth, and enhancing personal connectivity.

Risks to personal information like identity theft and privacy breaches increase annually as the world becomes more digital. The government of Alberta acknowledges that digital technologies create challenges to privacy and is committed to addressing those

challenges. The government of Alberta is exploring options to modernize Alberta's privacy protections to properly address the privacy concerns of Albertans and provide guidance on sound privacy practices. PIPA establishes the framework for private-sector organizations to enable innovation that is responsible and beneficial to consumers and society and ensures they can have their rights to privacy fully protected while enjoying the benefits of sharing their data with businesses.

Moving on to slide 8, Alberta is one of three provinces with provincial private-sector privacy legislation. As PIPA is reviewed, it is important to look at other Canadian and international jurisdictions and their legislation. I will first provide a comparison between PIPA and other private-sector privacy laws within Canada and then discuss the general trend of world-wide privacy law development and highlight a few major examples of privacy laws adopted by select countries.

Moving on to slide 9, as I mentioned, in Canada the Personal Information Protection and Electronic Documents Act applies to federal works, undertakings, and businesses. PIPEDA also applies to provincial organizations when they engage in commercial activity within Canada. Alberta organizations can be subject to more than one law, depending on what activities they are doing.

In June 2022 the government of Canada introduced Bill C-27 to modernize Canada's private-sector privacy framework through a proposed Consumer Privacy Protection Act, CPPA. The CPPA is a partial replacement of the current PIPEDA. Bill C-27 is the reworking of Bill C-11, the Digital Charter Implementation Act, which was introduced in November 2020 but did not proceed due to the announcement of the federal election. The intent of Bill C-27 is to strengthen Canada's private-sector privacy law, create rules for the responsible development and use of artificial intelligence, and continue advancing the implementation of Canada's digital charter.

The Standing Committee on Industry Technology, reviewing Bill C-27, completed hearings on February 14, 2024. In total, the committee held 22 hearings, receiving testimony from 85 different organizations and individuals as well as 98 written submissions. The committee is now conducting a clause-by-clause review of the bill, during which the opposition will have the opportunity to introduce motions to amend. Alberta's PIPA is deemed substantially similar to PIPEDA; therefore, PIPA applies to Alberta organizations. If passed, CPPA will likely impact the substantially similar status of PIPA. Technology and Innovation is engaged in ongoing discussions with the federal government in this regard.

Moving on to slide 10, like Alberta, British Columbia and Quebec both have their own provincial private-sector privacy laws, which are considered substantially similar to PIPEDA. The remaining 10 provinces and territories currently do not have specific private-sector privacy legislation, and therefore their private-sector organizations are subject to the federal PIPEDA. All three provincial private-sector laws – Alberta, B.C., and Quebec – apply to both consumer and employee personal information practices of organizations within each respective province with the exception of those that are otherwise governed by PIPEDA.

Both B.C. and Quebec recently completed a review of their respective privacy legislation. Quebec's Law 25 is an omnibus bill that amended 24 pieces of legislation that contain provisions related to the protection of personal information. The changes impact both private- and public-sector entities operating in Quebec, including businesses of all sizes, nonprofit organizations, and government bodies. The bulk of Quebec's new provisions went into effect on September 22, 2023, and introduced requirements for companies and organizations to publish comprehensive privacy policies, conduct mandatory privacy impact assessments, update privacy



notices and consent mechanisms, and adhere to rules regarding the destruction and removal of personal information.

The provisions in B.C.'s PIPA are broadly similar to Alberta's. However, unlike Alberta, B.C.'s PIPA applies to all private-sector organizations in the province that are not subject to PIPEDA. In April 2021 the Legislative Assembly of British Columbia appointed a special committee to review its PIPA. In December 2021 the special committee published a report with 34 recommendations. The committee concluded that PIPA must be modernized to safeguard rights for individuals and provide up-to-date provisions to ensure competitiveness for B.C. businesses. However, to date no amendments have been made in response to these recommendations.

Moving on to slide 11, at a global level over 130 countries have constitutional statements regarding the protection of privacy. Many countries have privacy legislation that governs citizens' information privacy rights and how organizations and agencies must handle personal information in relation to the collection, use, and disclosure. One example is the General Data Protection Regulation, or the GDPR, which is a European Union law with mandatory rules for how organizations and companies must use personal information in a secure and transparent way.

With innovative privacy measures such as the right to be forgotten, the GDPR has been a global leader in modernizing privacy legislation. Despite being an EU-driven law, it also has impacts for organizations world-wide. Other examples include Australia and New Zealand, which each have privacy legislation, whose scope varies across public and private sectors, to regulate the handling of personal information.

9:30

Moving on to slide 12, in the United States there is not a single national comprehensive data privacy and security law. The California Consumer Privacy Act and the California Privacy Rights Act are considered the most comprehensive privacy legislation in the country, and many states have patterned their laws after California's example. Since 2020 a total of 14 states – California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia – have passed state comprehensive privacy laws. Many other U.S. states have introduced or are in the process of reviewing state-level privacy legislation.

Moving on to slide 13, in closing, I would like to highlight three items. First, Alberta's PIPA has been deemed substantially similar to PIPEDA. This is important to keep in mind when thinking about potential amendments. It is also important as the changes to PIPEDA proposed by Bill C-27 may impact PIPA's substantially similar status.

Second, PIPA is often referred to as a consent-based legislation, which means that it primarily relies on consent for the collection, use, and disclosure of individuals' personal information. There are limited and specific exceptions to that requirement for consent.

Finally, the government of Alberta recognizes and embraces the move towards digital government while also acknowledging the challenges that digital technologies present for privacy. Protecting Alberta's privacy is a priority, and we have been exploring ways to adapt and modernize Alberta's privacy protections for the digital age.

Thank you for providing Technology and Innovation the opportunity to present.

**The Chair:** Thank you for your presentation.

Hon. members, we will now hear a technical briefing from the Information and Privacy Commissioner and her staff. You have 20 minutes for your presentation.

**Ms McLeod:** Good morning, Chair and members of the committee and ministry representatives. It's very nice to be here today to present our technical briefing on the Personal Information Protection Act. I'm excited by the work of this committee to review the Personal Information Protection Act.

Slide 2, please. Thank you. PIPA is an important law that provides a made-in-Alberta approach to privacy management for businesses that collect, use, or disclose personal information in the province. Its purpose is to balance the right of clients, customers, employees, and volunteers to have their personal information protected and the need of organizations to collect, use, or disclose personal information for purposes that are reasonable.

Privacy laws exist in this country to enable individuals to exercise control over their own personal information. The Supreme Court of Canada has stated that "the ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of [our] democracy." The court has characterized privacy legislation, which aims to protect individuals' control over personal information, to be quasi-constitutional because of the fundamental role privacy plays in the preservation of a free and democratic society.

Under PIPA individuals exercise control over their personal information through consent. What this means is that in general an organization cannot collect, use, or disclose an individual's personal information without their consent and can only do so for purposes that are reasonable. The additional rights afforded to Albertans under PIPA include the right to access their own personal information held by organizations, the right to request a correction to their own personal information, or to make a complaint about an organization that is not complying with the privacy provisions.

PIPA came into force in the province on January 1, 2004. It was drafted to make it practical for small and medium-sized Alberta businesses to implement. PIPA aims to protect the privacy of individuals who engage with organizations, including clients, customers, employees, donors, and volunteers, by establishing the rules for the collection, use, and disclosure of personal information by businesses and organizations in Alberta and requiring those businesses and organizations to have reasonable safeguards to protect that information such as by simply locking file cabinets or ensuring reasonable security measures are in place to keep hackers out of computer systems.

Slide 3, please. To ensure PIPA's purposes are achieved, I have a number of powers and responsibilities as commissioner, including reviewing whether businesses are complying with the act. An individual can make a complaint to my office if they believe an organization has improperly collected, used, or disclosed personal information or if the individual believes a business did not put in place reasonable safeguards to protect their personal information. An individual can also ask me to review the response received from an organization. If an individual is not pleased with the response they received after requesting access to their own personal information, I may also on my own motion conduct investigations to review an organization's compliance with PIPA, and I have order-making power under PIPA.

Orders can include requiring an organization to fulfill its obligations under the act such as responding to an access request or to stop some action that is in contravention of the act. For example, my office recently ordered a condominium corporation to stop posting without consent notices of arrears for residents in view of others as there are less intrusive ways to notify individuals that a debt is owed. Orders are enforceable in court and subject only to judicial review.

Since 2004 we have received more than 3,000 requests for review or privacy complaints under PIPA. A vast majority of those are resolved through informal mediation and investigation processes without the need for an inquiry, which is a formal hearing. Of the more than 3,000 reviews, approximately 208 have resulted in orders through the office's inquiry process.

Other responsibilities include reviewing privacy breach reports submitted by organizations, as required by PIPA when there is a real risk of significant harm to an individual affected by a breach. I can also order an organization to notify affected individuals if they have not done so already.

In the summer of 2022 my office issued a report that analyzed nearly 2,000 breaches reported to the office since 2010. Alberta was the leader in implementing mandatory breach reporting in 2010, which is now a common privacy protection globally. We have all been, or know someone who has been, victimized by a breach like when credit cards are hacked or e-mail lists are disclosed. I think that we can all agree knowing that a breach has occurred is an important right for Albertans so they can take steps to protect themselves from the harm.

Another important aspect of PIPA is that it requires a review by an all-party committee of the Legislative Assembly every six years, which leads us here today. I will now move from the technical aspects of the act to some of the higher level considerations and topics for potential amendments to PIPA that will be raised during this review.

Next slide, please. For this part of my presentation I start with a quote from the Supreme Court of Canada about PIPA. "PIPA's objective is increasingly significant in the modern context, where new technologies give organizations an almost unlimited capacity to collect personal information, analyze it, use it and communicate it to others for their own purposes." The Supreme Court has rightly stated PIPA's objective in the digital economy. However, because PIPA has not kept pace with digitization and the myriad of privacy implications of new technologies, its objective can no longer be achieved.

Over the past two decades the rise in the use of technology in the private sector has enabled organizations to amass a significant amount of personal information. In addition, the private sector is the primary developer of technology used in the public and health sectors to collect, use, disclose, and protect personal information. Today there are novel, cheap, and effective strategies malicious actors can deploy to try to exploit or steal digital assets, including personal information, from any organization that holds information. There is a marketplace on the dark web for the purchase and sale of personal information. Personal information is very lucrative to businesses and to thieves. Stringent controls are required to protect against these digital realities and threats.

With that in mind, this committee's work is timely and important in helping chart a new path forward for a modernized PIPA that supports Alberta's economic future while maintaining privacy protection for Albertans.

Next slide, please. Since the last PIPA review in 2015-16 there have been several significant changes to privacy legislation in recognition that the digital economy must be effectively regulated in order to flourish. Hilary covered some of that, and I will touch on it as well, briefly.

The European Union's General Data Protection Regulation, or the GDPR, came into force in May 2018 and impacts businesses around the world. In other parts of the world such as various U.S. states new privacy laws have been introduced. We are also seeing other Canadian jurisdictions pursuing legislative reform and modernization. Amendments to Quebec private-sector privacy law began coming into force in stages in September 2021 and will be fully implemented by September 2024. The federal government has

tabled Bill C-27 in 2022. The bill has passed first and second reading, and it is now undergoing consideration in committee. Bill C-27 includes the Consumer Privacy Protection Act, which would repeal and replace portions of PIPEDA, which is the current federal private-sector privacy law. Bill C-27 has elicited many commentaries to date. Finally, in 2021 the B.C. Legislature reviewed B.C.'s PIPA, with 34 recommendations for amendments.

9:40

The harmonization and modernization of law is important to many jurisdictions and to businesses that want certainty in this respect. Harmonization is of particular importance for the continued cross-border transfers of personal information to conduct business internationally. Without getting into specifics, Canada must maintain adequacy with the GDPR for trade to continue. Adequacy is a determination made by the European Commission on whether a country outside the EU offers an adequate level of data protection to European citizens. In turn, Alberta must maintain substantial similarity with the federal private-sector privacy law to oust the jurisdiction of PIPEDA in the province.

These realities underscore the need to update PIPA with both a national and a global lens. In addition, updating the legislation to address the new realities of the risk to privacy caused by technological innovation ensures that the privacy rights afforded to Albertans under PIPA are on par with residents in other parts of Canada and globally.

Next slide, please. Among the changes in the new and amended privacy laws, individuals have been given rights respecting automated decision-making. In other words, if a decision is made about or for an individual by a piece of software or bot using machine learning or artificial intelligence without human involvement, then recourse becomes available to the individual. These rights recognize the harms that can occur to an individual through automated decision-making technology such as decisions to deny a loan or insurance.

In GDPR, for example, there is a right for individuals to receive information about the automated decision being made and a right for individuals to object to a decision, challenge a decision, or seek human intervention. These rights apply in limited circumstances such as when a business is carrying out automated decision-making without human involvement that has legal or similarly significant effects on an individual.

Another approach to automated decision-making is in the California Consumer Privacy Act, which requires businesses, in response to access requests, to include meaningful information about the logic involved in those decision-making processes as well as a description of the likely outcome of the process with respect to the consumer. There is also a right to opt out of an automated decision. The rules for applying these rights in California went into effect on January 1, 2023.

Many commentators are asking for regulations to align with GDPR and other laws concerning artificial intelligence. Modernized legislation is also requiring businesses to have privacy management programs that are scalable to the nature of their business. Privacy management programs were a concept developed by Canadian commissioners in Alberta, British Columbia, and federally, but other jurisdictions have been the first to introduce privacy management programs and legislation. The other theme with new and modernized laws is more effective enforcement measures for commissioners and other privacy regulators.

Without getting into the legal specifics of today's remarks, these and many other changes have all been significant. To get up to speed, organizations invested heavily in preparing for and maintaining compliance with GDPR, Quebec's private-sector

privacy law, and other new privacy laws. As a result, many businesses need to consider the higher privacy protection thresholds in other jurisdictions, which leaves Alberta's PIPA behind. To ensure PIPA's continued relevance as a made-in-Alberta approach, it will need changes that reflect what has occurred elsewhere with respect to privacy regulation and enforcement.

Next slide, please. Another impetus for amendments to PIPA is that a trust deficit has accumulated between customers and businesses with respect to privacy. A number of stories have eroded people's faith in the protection of their privacy in the digital economy, which has reinforced the need for stronger legal protections. Maintaining public trust goes to the heart of facilitating a digital economy. An example is the work we did in investigating PORTpass. You may recall that PORTpass said it could provide a mechanism for proof of vaccination for entry into one of the Calgary Flames games. During the investigation, however, PORTpass failed to demonstrate that it implemented any technical administrative safeguards to protect personal information, as required by PIPA.

We also teamed up with our private-sector privacy colleagues in Canada on two investigations. One was our investigation with Quebec, B.C., and the federal commissioner's office into the Tim Hortons app, which found that Tim Hortons was collecting vast amounts of sensitive location data even when the app was not being used. The second investigation with B.C. and our federal colleagues was Cadillac Fairview, the operator of shopping centres, and its use of facial recognition software at information kiosks without consumers' consent. Both investigations resulted in widespread media coverage and found the companies did not comply with Canadian private-sector privacy laws. In our work reviewing breach reports, we also started seeing significant increases in phishing incidents and ransomware breaches, from a handful to hundreds of reports each year.

These and many other stories raise society's awareness about the understanding of privacy issues. There was a sudden increase in topics like algorithmic transparency, cybersecurity, data brokers, targeted advertising, and profiling being covered by mainstream media. Algorithmic transparency, for example, is at its core about letting individuals know the logic involved when a machine makes a decision using artificial intelligence.

We also saw some stories where improper handling of personal information or deceptive practices involving personal information destroyed the reputation of some companies and generally decreased confidence and trust in businesses that handle massive amounts of personal information. Businesses stockpiling personal information for potential market use or bad actors that exploit security vulnerabilities to steal personal information are just some of the risks to personal information. The stories told and risks exposed reinforce the need for strong, modern legal protections.

Next slide, please. This is why I was pleased to read the message that the hon. Nate Glubish, then minister of service Alberta, issued on January 28, 2022, on Data Privacy Day. The minister wrote that Alberta's review of privacy laws must centre on two core principles, strengthening privacy protections and building trust. More recently, on Data Privacy Day this past January Technology and Innovation Minister Glubish made the following comments when announcing two frameworks for use by government to better protect the personal information of Albertans.

Albertans should have the strongest privacy protections in Canada. Every service we provide, every technology we build, every tool we deploy to modernize government systems and services will adhere to the principles in these frameworks.

The privacy of Albertans is non-negotiable. Come hell or high water, I'm here to protect it.

I was pleased to see the minister's support of the concepts of privacy by design and ethics by design to guide the development of new technologies and proposed amendments to the legislation.

Taken together, we now have the benefit of more evidence to support amending PIPA to align with today's digital economy and Alberta's desire for diversification such as through fintech and other data-driven technologies. Regulators, governments, and businesses all play a role to make up the trust deficit that currently exists between consumers and organizations. To do this effectively, we need a modern law that enhances Albertans' privacy rights, reflects the digital information economy in which Alberta businesses are competing globally, and introduces effective enforcement measures that incentivize compliance, as opposed to the current model that has no significant consequences for noncompliance.

With respect to the information economy something else that must be considered during the PIPA review is the increased digitization in Alberta's public and health sectors. As we move towards better broadband Internet for rural and northern Alberta, work to meet societal demands for enhanced digital public services, and focus on virtual health care delivery, we must recognize that public- and health-sector innovation goals are reliant on private-sector products and tools. For example, there are many potential opportunities to leverage public- or health-sector data to drive private-sector innovation through cross-sector information sharing. These are laudable ideals that are worth exploring, but keep in mind that these types of projects must prioritize protecting Albertans' personal and health information or risk failing altogether.

We also see the convergence of the private and health sector through privacy impact assessment reviews that involve the development of apps by the private sector that are marketed to custodians to support the delivery of health care in Alberta and investigations of virtual health care solutions under the Health Information Act. These examples highlight the need to consider how Alberta's three privacy laws work together to ensure there are adequate protections in place to facilitate responsible and effective data-driven innovations.

9:50

Next slide, please. The key message I have today is that without a thorough review of PIPA and comprehensive proposed amendments, PIPA is at risk of falling further behind and not adequately protecting the personal information of Albertans, especially as businesses continue to leverage digital solutions in service offerings to customers and for marketing to the public and health sectors. We need to remain attuned to the various factors contributing to the need for change, including legislation reform globally and within Canada, the trust deficit between consumers and businesses, and the convergence of the public- and health-sector goals with private-sector innovations.

With that, I conclude by saying that private-sector privacy compliance and regulation remains a paradox. The only constant is change, driven mostly by digitization. As a society we now recognize how vulnerable and how valuable our personal information has become and that there are risks to our person and to our rights and freedoms when our privacy is not adequately protected. It is for this and many other reasons we need to seriously reflect on how PIPA must operate now and in the years ahead, a made-in-Alberta law that reflects a modern digital economy, protects Albertans' personal information, and builds trust in businesses.

Thank you.

**The Chair:** Thank you for your presentation.

I'd like to open the floor now for questions of both the ministry and the Information and Privacy Commissioner. We'll kind of go back and forth as we ask the questions, and you can ask the question and have a follow-up based on the answer, and then we'll go over to the next side. We are able to start now, whoever wants to start.

**Mr. Eggen:** Thanks for your presentations. There are a number of issues around technology that I just wanted to ask about, the first being facial recognition technology. First, do we have specific legislation or protections or constraints around using facial recognition technology? If you could provide a recommendation of where we could perhaps buttress protections for the public against using facial recognition technology. Like, you mentioned the Cadillac Fairview issue that came up last year, I think.

**Ms McLeod:** Is that directed towards me?

**Mr. Eggen:** Yes.

**Ms McLeod:** Okay. Under the Personal Information Protection Act the definition of personal information includes biometrics, so there is some specific reference in the Personal Information Protection Act. However, it's not regulated specifically for biometrics but is taken into consideration in the broader provisions of collection, use, disclosure protection under the act. What we are looking at doing is making recommendations to potentially identify certain kinds of information as being more sensitive than others. Biometrics would be one of them. As part of our recommendations to amend PIPA – in fact, we are looking at the FOIP Act as well as HIA at the same time, and we are making similar recommendations about defining certain categories of sensitive information that would include biometric information, as I indicated.

Do either of you want to add anything to that? Okay.

**Mr. Eggen:** Would you extend that recommendation not just to a private entity like Cadillac Fairview and so forth but also for the use by police and law enforcement?

**Ms McLeod:** Yes. Under the FOIP Act as well, which law enforcement is subject to, and the Health Information Act, which custodians are subject to.

I'll just take a quick moment to say that it's the 23rd anniversary of the Health Information Act today.

**The Chair:** Thank you very much.

We'll go to Member McDougall.

**Mr. McDougall:** Thank you for your presentation today. You touched on, you know, an inherent need to balance the responsibility of individual private rights, making sure that they're protected and secure, versus the desire to reduce cumbersome red tape or, in many cases, actually, through technology reduce red tape. That's part of the application or one of the advantages of data management. There's a bit of a balance there. I think the issue is balance. How does PIPA manage to do both of these things? How do you balance those two things, exactly? What is the criteria that's used? They are sometimes contradictory but somehow has to be negotiated between them.

**Ms McLeod:** Is that question for me?

**Mr. McDougall:** I would say yourself or Hilary.

**Ms McLeod:** Okay. Sure. Well, the way that it's balanced in PIPA is that it actually facilitates the use of personal information by businesses for reasonable purposes with consent. So it does enable

businesses to use personal information for their own purposes, including to generate profit, so long as it follows the rules in PIPA. Then the rules in PIPA that apply to privacy allow an individual to control their own personal information in that engagement with the private-sector business. So it differs significantly from, for example, the Health Information Act, which actually focuses on the centre of care or the circle of care and then the controls that go along with that.

FOIP is not consent-based legislation. It recognizes the fact that individuals really cannot consent to the services of government. That's why private-sector privacy legislation works on the consent model, and it achieves that balance between an individual's right to control their information with that particular service and an organization's ability to use it for legitimate business purposes or reasonable purposes, as it says in our act.

**Mr. McDougall:** We talk about control. I noticed that in the definition of privacy it's "some control," and I guess the question is: some. Again, there's a range of what "some" means. Is there a way to provide some indication as to exactly what some control is applied to? And, you know, what are the criteria for more control or less control?

**Ms McLeod:** I'm not sure what you're referring to. I can answer it in the way I understand the legislation works as it relates to control. The legislation itself is designed to facilitate that control over one's own personal information; it's the provisions themselves that enable that control. In PIPA I would say that there is a stronger kind of control because it's consent-based legislation. Because I'm dealing with the private sector, I have a choice of shopping around. I don't have to buy anything from you; I can buy it from you. That's why it's consent based, and that's how I exercise control. But the provisions themselves actually are designed to give control depending on the context. In FOIP you exercise control in a certain way, in HIA you exercise control in a certain way, and in PIPA you exercise control in a certain way. I wouldn't call it: some control. I would call it: that's what the provisions are doing.

**Ms Faulkner:** I think you may be also speaking to the definition on the first slide of the presentation I gave. The reason we used "some" there was to accommodate for those instances when an organization may be able to use or disclose information without consent. We wanted to be able to – I don't know – be as accurate as possible when we're describing that definition at a high level. There are cases when an organization, like, if they're required by law to provide that information, which – an individual would not necessarily give consent in that situation because there would be a statute or legislation that would override or be the, I guess, reason that an organization would have to provide that.

**Mr. McDougall:** So looking forward to amendments to legislation that exists today and particularly in terms of government-acquired information – health would stand out as this type of thing – do we anticipate that, you know, with information that's going to be obligatorily provided to the government, there will be control by the individual as to what is done with that information in terms of what it's going to be used for and how? Again, where's the line there?

**Ms Faulkner:** In that instance, as the commissioner mentioned, the government's collection, use, and disclosure of information is under the Freedom of Information and Protection of Privacy Act. As part of, I guess, broader work to modernize privacy protections, that is one of the pieces of legislation that the ministers of

Technology and Innovation and Service Alberta and Red Tape Reduction are exploring.

**10:00**

I'm not sure I fully understand your question in terms of what measures would be addressed. But under the legislation currently the section clearly outlines when the government or public bodies can collect information and under what authorities we can do so.

**Ms McLeod:** I could provide some clarity around that. Under FOIP it's not a consent-based model. There are three circumstances that permit a public body to collect information, and one of them, the most common, is "a program or activity of the public body." As part of that, a government is obligated to actually collect information directly from an individual, and as part of that, they have to provide notices about the purposes of collection and use. That is the control that's built into the Freedom of Information and Protection of Privacy Act, and if they're collecting indirectly, then the default is that they actually have to get consent. So the control is built into the provisions.

**The Chair:** Maybe we'll come back next time. Okay.  
Next one is Member Al-Guneid. Go ahead.

**Ms Al-Guneid:** Yeah. Thank you for your presentations. I did appreciate your comparisons to other jurisdictions and to Europe. At the same time, I heard references to a made-in-Alberta PIPA or laws, and I'm just curious if you can summarize what is uniquely made in Alberta here. Like, I mean, the whole world is facing the same challenges, the trust deficiency, the facial recognition techniques. All these are happening across the world. I'm curious what would be uniquely Albertan here.

**Ms McLeod:** Thank you for the question. As I had mentioned at the last technical briefing I did, Alberta is in the very unique position in Canada to have three pieces of legislation governing the health sector, the public sector, and the private sector. As we move ahead with some of the innovation that's happening in the province – and, as you all know, Alberta is one of the global leaders on technological innovation, including the development of artificial intelligence – what we're seeing here is that there's an interplay between the three pieces of legislation. So what I consider to be uniquely Albertan is the ability to actually harmonize our three laws to facilitate the sharing of innovation and the use of the information for technological advancement but still building in adequate privacy protections for Albertans under the three particular pieces of law. What that means is: identifying certain kinds of definitions that are standard; understanding, you know, how information is shared and what those rules look like in the circumstances; beefing up the research provisions and accountabilities in the laws.

Then going back to something that's more unique to Alberta than other provinces and territories, for example, we have order-making power under our legislation. So we have quite a bit of authority to enforce the compliance with the act. Some of the other things that I would like to see in our new legislation across the board, including PIPA, is more accountability or responsibility for the Privacy Commissioner to actually support the compliance by our various businesses in the province. That's what I would say about it being uniquely Albertan.

The ministry might have something to add to that.

**Ms Faulkner:** I think when the legislation was first introduced, it was, I guess, looked at as kind of leading legislation across Canada. In terms of being, I guess, uniquely Albertan or made in Alberta, the connection, too, for me goes to the substantially similar status.

It allows Alberta to have its own privacy legislation and not necessarily, like other provinces and territories, have the private sector follow the federal legislation.

**Ms Al-Guneid:** Yeah. I mean, I appreciate that, and I'm curious if you've looked at Quebec's. I mean, really, Quebec is the leader on AI and the whole machine learning space. They have Mila, the Mila AI institute. I remember that five years ago I did a tour with my previous job, and they had a whole building just on AI ethics and privacy. I'm just challenging the idea that this is all uniquely Albertan. There's a lot to learn from other jurisdictions that are leading the way in this space, and I would encourage you to look at what these jurisdictions are doing there.

Thank you.

**The Chair:** Any comment, or that's good? Okay.  
Did you want to carry on, Member McDougall?

**Mr. McDougall:** We'll let somebody else go.

**The Chair:** Okay.  
Is there anyone else? Member Bouchard, go ahead.

**Mr. Bouchard:** Thank you, Chair. We understand that the technology climate has been rapidly evolving in Alberta and around the world for a number of years now. It's come with changes to the information and privacy landscapes, of course. In the view of the ministry has PIPA continued to perform at an adequate level, providing Albertans with a strong level of information protection?

**Ms Faulkner:** In terms of, I guess, since 2004, as I mentioned when I went over the history, there have been amendments, various amendments, along the way. In the last, I'd say, maybe five to 10 years we've really seen the evolution of technology and data use at a pace that has previously maybe not been there, and with that does come the need to modernize PIPA in certain ways. There are many things in PIPA already that I would say are already excellent, and any kind of modernizations are really recognizing the changing technology ecosystem that we're seeing for Albertans. The commissioner has commented on a few things, and the department would be happy to provide a submission to the committee if that is of interest.

**Mr. Bouchard:** Okay. Thanks.  
No follow-up.

**The Chair:** Okay.  
Any others? Go ahead, Member Eggen.

**Mr. Eggen:** One, I think, area of concern for myself and for everyone, really, is the integrity and the privacy of health records. You know, the importance of public health care is not just that people can access care not based on how much money they have but on their needs for health care. Another area is in the area of insurance for accessing certain procedures. As Alberta unfortunately descends into more privatized health care, I'm very concerned that the integrity of the privacy of an individual's health records is maintained and buttressed somehow through privacy legislation. If insurers get access to preconditions and so forth, they can perhaps not insure someone or someone can be left without being able to access the health care that they need. I'm just wondering if any of you have been thinking about that, and what can we do to strengthen the privacy around people's health records?

**Ms McLeod:** Well, the records that we're talking about are under the Health Information Act, not under the Personal Information

Protection Act, but there are strong controls under the Health Information Act for the protection of health information. We're currently in conversation with the Ministry of Health, Alberta Health Services, and a number of other people in the province about health information and how it can be adequately protected. So we are thinking about that.

Of course, the insurance factor is an issue not only in the health sector but also under PIPA. PIPA actually does regulate a number of noncustodian health care providers. You know, information is sensitive there in some circumstances as it relates to the ability to get insurance if information were breached, for example. So the controls need to be adequate across the board to ensure that there are adequate levels of protection of particularly sensitive information which can actually cause harm to individuals if it's breached.

**Mr. Eggen:** So you might suggest that working more closely with Alberta Health Services to build amendments to PIPA to protect individuals' health care records would be a good idea?

**Ms McLeod:** Yes. I am talking to them about that under the Health Information Act, but as I said, PIPA needs to have those strong controls across the board. I think one of the members here mentioned the fact that we have a significant amount of health information centralized in one custodian, and I think that as far as our data holding goes, that's a global standard, that we have the most in one place. And I can assure you that there are many researchers and developers that are looking to get their hands on that data to actually develop artificial intelligence that they can then market. So, you know, we're looking very closely at those issues and trying to figure out how best we can facilitate certain amounts of innovation while adequately protecting the health information of Albertans.

10:10

**Mr. Eggen:** Absolutely. And probably it underlines the importance of this committee to have access to that information as you're working with Alberta Health Services and other bodies, for sure.

**Ms McLeod:** Yes. I'm happy to relay sort of the ecosystem that I'm looking at trying to develop. As Hilary mentioned, we would also be pleased to provide a submission to the committee and answer any questions that they may have as you work through your review of PIPA.

**Mr. Eggen:** Yeah. That's a good idea.  
Thank you.

**The Chair:** Thank you.  
Member van Dijken.

**Mr. van Dijken:** Okay. Thank you, Chair. My first question is for the ministry regarding the appeals process on decisions. Some jurisdictions have fairly formalized appeals process mechanisms. The primary option in Alberta is judicial review. I'm looking for possibly details, any insight on the criteria that would have to be met and the process to be followed for a complainant or an organization, I guess, to apply for a judicial review with regard to the commissioner's order.

**Ms Faulkner:** I would actually maybe pass that to the commissioner to answer.

**Mr. van Dijken:** Okay. Fair enough.

**Ms McLeod:** Yeah. I mean, under the act – I don't have all the particulars in front of me, and I can certainly get that information back to you – once an order is issued, I believe they have 50 days to appeal to the Court of King's Bench. Yeah. I think that's pretty much it. Was there something more that you were wondering about there?

**Mr. van Dijken:** Okay. If I may, Chair?

**The Chair:** Yep.

**Mr. van Dijken:** So, then, they ask for an appeal, and it's automatically granted, or there would be a determination, I'm thinking. Like, it wouldn't automatically go to a judicial review, I wouldn't think.

**Ms McLeod:** Well, it's up to the court at that point. You know, we don't have any involvement in that. Actually, we did have a situation recently where a court refused a judicial review, but generally they do go forward. But it takes years to happen.

**Mr. van Dijken:** Just for my clarification, I guess, I would have one question on whether or not the commissioner is able to have full standing within a judicial review and be able to present at a judicial review.

**Ms McLeod:** I'm not an expert on this part of the equation, but we do have standing during judicial reviews. I just don't know exactly what that looks like. But, again, I can get you some more detail, if you'd like, around sort of what that process looks like.

**Mr. van Dijken:** If we need it, I think we will probably get some more information on that as we talk. Yeah.  
Thank you.

**Ms McLeod:** Okay.

**The Chair:** Any others? Go ahead, MLA Armstrong-Homeniuk.

**Ms Armstrong-Homeniuk:** Thank you, Chair. Through you to – I can't see that far. Is it Diane?

**Ms McLeod:** Me?

**Ms Armstrong-Homeniuk:** Yes.

**Ms McLeod:** Yeah. It's Diane.

**Ms Armstrong-Homeniuk:** Thanks. I can't see that far with my glasses.

One of the issues myself and, I'm sure, others on the committee have been hearing a lot about in recent years is about companies selling information and data to their customers or users, and I'm wondering what types of protections exist in the act for the users of social media sites and the like to have their data protected. We see a lot of that lately.

**Ms McLeod:** For social media sites specifically?

**Ms Armstrong-Homeniuk:** Yes.

**Ms McLeod:** PIPA applies to any information that's collected in Alberta. Let's just use Facebook as an example. If they're collecting information from people that are in Alberta when the collection occurs, then PIPA does apply. So that means that any collection, use, and disclosure rules would be – Facebook would have to comply with our legislation as it relates to those.

**Ms Armstrong-Homeniuk:** How would this work if a person had a VPN even though they were in Alberta, but they use a VPN for Saskatchewan or B.C.? Would PIPA apply to that, too?

**Ms McLeod:** It would apply to any information that's collected in Alberta by an organization as that term is defined in the legislation. The VPN might be more of an employee kind of channel. In that case, you know, it would apply as employee information, but it would have to be personal information, and a lot of work-related information is not considered personal information because it's work product. If it's collected in Alberta, PIPA applies to it.

**Ms Armstrong-Homeniuk:** Okay. Thank you.

**The Chair:** Any on the opposition side? Okay. Good.  
MLA Hunter.

**Mr. Hunter:** Thank you, Mr. Chair, and thank you for being here this morning as we discuss these important matters. Not too long ago, NDP MLA Thomas Dang hacked into the health care system and looked for . . .

**Mr. Schmidt:** Point of order, Mr. Chair.

**The Chair:** A point of order.

**Mr. Schmidt:** I raise a point of order under Standing Order 23(b), speaks to the matter "other than the question under discussion." We know that the matter that Member Hunter is referring to was a violation of the Health Information Act. We are here to discuss the protection of information and privacy act, so I ask that you rule this question out of order. Thank you.

**Mr. Hunter:** Mr. Chair, I think that this is very relevant. If I had the opportunity to be able to finish the question, it would have been: have we been able to shore up these holes to make sure that this sort of thing doesn't happen? I think that that's very relevant to the questions at hand, so I hope that this is not considered as out of order.

**The Chair:** Well, as opposed to using the name, if we can talk about pushing, you know – like the holes you talked about: just getting the holes fenced up. For breaches, like how breaches are handled: if you could handle it that way, that would be great.

**Mr. Hunter:** Well, Mr. Chair, if I might. I know that this is a prickly matter for the members opposite, and I'm not saying that they had anything to do with this, but I'm just saying that a member from the NDP MLA caucus did do this. It's a matter of record. And the question that I had to ask was: have we been able to shore up? This is what this whole thing is about, protecting people's privacy.

**Mr. Schmidt:** Yeah. Mr. Chair – Mr. Chair – again, a point of order.

**Mr. Hunter:** Excuse me, Mr. Chair. I'm actually speaking right now.

**Mr. Schmidt:** Yeah. Listen. He has ruled. Now I get to raise a point of order, Mr. Hunter.

**Mr. Hunter:** I hadn't actually finished, Mr. Chair.

**The Chair:** Okay. I'd like to have him finish, and then when he's finished, we can do the point of order.

**Mr. Hunter:** So what I was saying is that I think that it's important to be able to understand whether or not we've been able to shore up this information, these gaps that were in PIPA, if it was in PIPA. If it's not, then I needed to understand that. That was the only purpose for being able to ask this question. Thank you, Mr. Chair.

**The Chair:** Okay. I will allow you to answer the question based on: if it's not in PIPA, then fine; if it is, then if you could answer it.

**Ms McLeod:** No, I understand the question. Thank you.

Your question is about: is PIPA adequate enough to ensure adequate security? I think the answer to that is: it depends. Every organization will interpret the reasonable security arrangements, requirements in PIPA on its own, and there are differing interpretations, and sometimes those interpretations lead to significant security risks. The other thing that is at issue is the fact that there is no incentive to comply with PIPA. There are no real consequences for not complying with PIPA. And if you're looking at it from an enterprise risk perspective, which most organizations do, you're going to put that cost low on your bar, because there is no cost to a breach other than potential reputational harm.

What we're seeing, the way the legislation is structured without adequate consequences and deterrence for compliance, is actually noncompliance, and that creates security risks, and that is a vulnerability for Albertans. What we would be looking at for amendments that we would put forward in our submissions is strengthening the security requirements in the act and increasing the enforcement opportunities for the commissioner to deter compliance, which will then, or theoretically should, shore up the security to adequately protect from breaches, which, as we know, can cause significant harm to people.

**Mr. Hunter:** Thank you, Mr. Chair. I appreciate the answer.

**The Chair:** Thank you very much. Any others?

Okay. If there are no other questions, I would like to thank the representatives from the Ministry of Technology and Innovation and the office of the Privacy Commissioner for providing their presentation and responding to members' questions. You're welcome to remain if you want, or if you need to leave, that's okay, but you're welcome to stay either where you are or up in the bleachers if you want. Thank you very much.

**10:20**

Okay. At our first meeting on January 22 the committee tasked LAO research services with some research items to help the committee with its review of the Personal Information Protection Act. Each of the items has been made available to committee members on the internal committee website. Dr. Christina Williamson is here to give an overview of each for the committee.

**Dr. Williamson:** Thank you very much, Mr. Chair, and good morning to all the members of the committee. Thank you so much for being here. This morning I'm actually presenting three distinct research products, so I'll try and be brief. I know it's a long meeting, but it is a very important piece of legislation, as you've all pointed out. As mentioned by our technical briefs, PIPA is part of a changing landscape of the private-sector privacy legislation world.

The crossjurisdictional here: we tried to keep it short and sweet. Sorry. It's not. It's under 100 pages though. It tries to provide a really robust view for the committee of this law in Alberta. This crossjurisdictional discusses legislation provincially in Canada, federally as well as in Europe. I'm not going to go into too much detail of the breakdown of the document, but I do want to talk a

little bit about the various laws that are covered under this crossjurisdictional.

The report covers the three existing provincial level private-sector laws. The ones in Alberta and B.C. are quite similar. They're both called PIPA, and they were, I think, also proclaimed in the same year, in 2004. Also, Quebec's *Loi sur la protection des renseignements personnels dans le secteur privé* was also discussed in our technical briefings. This is currently the most up-to-date legislation that exists provincially in Canada.

Federally, there is coverage for all the provinces without their own distinct privacy law. Currently, as noted before, it is the Personal Information Protection and Electronic Documents Act, PIPEDA. What's really notable about this right now is, of course, Bill C-27, the Digital Charter Implementation Act, which is currently at the committee stage, the report-writing stage, in the House of Commons. We're just kind of waiting on that report to see what the recommendations of that committee will be. Bill C-27 contains three separate statutes: the Consumer Privacy Protection Act, which will replace portions of PIPEDA. There's also the Personal Information and Data Protection Tribunal Act, which may create a tribunal system and will be responsible for inquiries, issuing compliance orders, and issuing administrative penalties and fines. Finally, Bill C-27 also includes AIDA, which is the Artificial Intelligence and Data Act, which will likely regulate the use of AI, artificial intelligence, here in Canada.

And last but not least, the crossjurisdictional discusses and includes the European Union's General Data Protection Regulation, known as GDPR. GDPR is included in this crossjurisdictional because it is the international model for privacy legislation, and as noted before, there are adequacy requirements for any corporation that processes any data of an individual who is located in Europe. So it's quite a high threshold, and there are impacts on corporations here in Alberta that might process data of people in the EU.

I'll also note that the U.K. kept the GDPR once it left the European Union, so there's also a little bit of discussion about the U.K. GDPR, which is virtually identical.

I'll just stop there. Thank you so much.

**The Chair:** Yeah. Okay. Well, thank you very much.

Do members have any questions relative to the crossjurisdictional report? MLA Armstrong-Homeniuk. I got it that time.

**Ms Armstrong-Homeniuk:** Thank you. How long do I have, Chair?

**The Chair:** Well . . .

**Ms Armstrong-Homeniuk:** As long as it takes? Okay.

Thank you, Chair. Through you, Chair, to Christina and your group. I don't know who would answer this one, but I see that the CPPA would be somewhat unique amongst the jurisdictions listed in the crossjurisdictional comparison in that it provides a mechanism for complaints and organizations to appeal the commissioner's decisions to a tribunal. Are there similar mechanisms or other bodies that fill similar functions in other jurisdictions analyzed?

**Dr. Williamson:** I can maybe answer a little bit, because we have a number of experts in the room.

**Ms Armstrong-Homeniuk:** Okay.

**Dr. Williamson:** To my knowledge this is the first time such a structure has been potentially proposed and implemented, but maybe the commissioner has a comment.

**Ms Armstrong-Homeniuk:** Sure.

**Ms McLeod:** Yes. I would concur with your response, actually. I think that the advent of the tribunal has a lot to do with the inclusion of administrative monetary penalties by the Privacy Commissioner, so they can appeal to this tribunal as part of that mechanism. But it is unique in Quebec. The commission can actually issue administrative monetary penalties directly without a tribunal appeal mechanism.

**Ms Armstrong-Homeniuk:** Okay. Thank you.

**Dr. Williamson:** Thank you.

**The Chair:** Any on the opposition side? No.

Any others on the government side? If not – you're okay?

**Mr. McDougall:** I'll ask a question.

**The Chair:** Okay.

**Mr. McDougall:** You talked about how the GDPR – or it's been discussed how the GDPR is impacting other jurisdictions. I can speculate a little bit as to how that might be, but I guess I would be interested to know a little bit more specifically, you know, how exactly is what's being legislated in another jurisdiction affecting us and requiring us to respond in kind or even be similar to what another jurisdiction has determined.

**Dr. Williamson:** Certainly. Great question. You're referring to what is called the extraterritorial effect of the GDPR. I think this was quite a novel reality of this law. It wasn't something that had been really tried before. But you'll see, if you go onto a website: do you want all the cookies to apply? That is an impact of the GDPR on us. A lot of corporations just said: well, it's just easier to apply this across the board rather than to only apply it to people located in the European Union. That speaks to the adequacy requirement that often plays out for corporations, where they go: well, it's probably easiest to harmonize to the highest threshold. In Quebec the response was to try and adjust the law so that it better aligned with the GDPR's requirements as well to simplify things for corporations.

I don't know if you want to add any more.

**Ms McLeod:** Yeah, that was a good response.

**Dr. Williamson:** Thank you.

**Ms McLeod:** The GDPR actually affects our ability to have trade with the European Union, and if we don't have adequacy standing, as determined by the European Commission, then it can actually cut off trade with Europe, which is why GDPR is having such an effect on Canada and also the United States. They're trying to amend the federal privacy legislation to meet that adequacy requirement so that it can maintain that standard to ensure that we can facilitate trade with Europe.

**Mr. McDougall:** Thank you.

**The Chair:** MLA van Dijken, go ahead.

**Mr. van Dijken:** Yeah. I don't know exactly if this falls in the crossjurisdictional report or who is best to answer the question. I guess the act defines "reasonable" as what "a reasonable person would consider appropriate in [the given] circumstances." Is that definition fairly similar through all jurisdictions? Has anybody come up with a better definition that would be more clearly defined? I'm not sure who's . . .



**Dr. Williamson:** Mr. Chair, could I defer that question to the commissioner?

**Ms McLeod:** Okay. You know, I don't know, actually, if it is the same as in B.C.'s Personal Information Protection Act. I expect that it might be because our laws were drafted basically together. I know that in the new CPPA I do not believe they're using this reasonable standard. They have different kinds of authorities to collect information under that piece of legislation. Unfortunately, I can't say for sure across the – but there are only four. There's Quebec, B.C., Alberta, and then the federal legislation.

**Mr. van Dijken:** Right.

**Ms McLeod:** I don't know what Quebec's is, but I can find the answer for you if you like.

**Mr. van Dijken:** If I may, Chair.

**The Chair:** Yeah. Go ahead.

**Mr. van Dijken:** If the commissioner has a recommendation that could more clearly define it, then I think we'd be open to receiving a new definition.

10:30

**Ms McLeod:** My colleague has a response.

**Mr. Stinner:** Yeah. What I can say is that in having worked with other jurisdictions a fair bit, there are similar – the wording changes, but the idea is the same: appropriate, reasonable. The alignment is there right now, which I think speaks to the fact that those laws have been recognized as being substantially similar.

What I will add, if I may, is, you know, something maybe for the committee to think over, the increasing complexity that I think arises from the increasingly interconnected nature of the digital economy. It impacts that. That is a fundamental change here. The increasingly connected nature of the digital economy impacts the complexity, the extraterritorial effect of laws. That is a fundamental change here that I think is really important for the committee to consider.

**Mr. van Dijken:** Just a follow-up on that comment. I guess my question would be on "reasonable," then, a "reasonable" person. Does that change over time based on complexity, based on differing circumstances, based on technology, all of these things? Is that level of determination evolving, and is that why the definition cannot be nailed down?

**Ms Stelmack:** Yeah. I think that's very fair to say. It's quite contextual. It's supposed to be objective. It's like the reasonable person off the street. It's a standard that's also used in tort law, for example.

**Mr. van Dijken:** Thank you.

**The Chair:** Thank you very much.

Any others?

Okay. The next research item prepared for today's meeting is a document that identifies emerging issues related to privacy legislation so that the committee members are aware of their potential impact. I will turn the floor over to Dr. Williamson to go over this document.

**Dr. Williamson:** Thank you again, Mr. Chair, and hello, members. We also produced this document we're calling the Emerging Issues document. It's a sort of discussion guide, but it also helps fill in

some of the spaces because of the reality of PIPA. As noted earlier, PIPA was written in a technologically neutral way in 2004, and certain technologies and the use of personal information in the digital economy simply were not really conceivable in 2004, so there are these gaps in the law as a result.

This Emerging Issues document allowed us to have an opportunity to discuss some of those issues such as artificial intelligence, the digital economy. The document also discusses the application of PIPA to nonprofit organizations and political parties; protection of sensitive personal information – that was around biometrics, whether that is a type of information that might deserve different levels of protection compared to, say, a phone number – safeguarding personal information in general; breach notifications, which has also been brought up by the committee before; and then administrative monetary penalties.

This document also includes a series of questions at the end of each section, which is an attempt to prompt people to think a little bit about how these issues might look within an amended PIPA. I hope this document will support and be helpful for the committee in this work. The committee in, I think, the next agenda item might want to consider including this document in its invitation letters to stakeholders. This might be a useful document for soliciting feedback from stakeholders and help frame the discussion and the conversation.

On that note, thank you very much.

**The Chair:** Thank you very much again.

Does anyone have any questions relative to the Emerging Issues document?

**Mr. Bouchard:** I'll go, Chair.

**The Chair:** Okay. Member Bouchard, go ahead.

**Mr. Bouchard:** Thank you. The Emerging Issues document mentions that the GDPR has an extraterritorial effect in that it applies essentially to any organizations that operate in any capacity in the EU regardless of whether the personal data being processed is in the EU. Have there been any domestic advantages for the EU from the approach that you're aware of?

**Dr. Williamson:** No. I'm not sure I can comment on that particular question.

I don't know if anyone over there might.

**Ms McLeod:** Actually, we have a similar effect under our legislation, under PIPA. We have mandatory breach reporting, and if the information was collected in Alberta – it doesn't matter where it was collected. If it was collected in the United Kingdom, for example, and it was collected online in Alberta, then our legislation applies, and they have an obligation to report to us. So we get breach reports from all over the world.

**Mr. Bouchard:** Thanks.

**The Chair:** Any others? Member McDougall, go ahead.

**Mr. McDougall:** Yes. It was alluded to earlier today, the issue of AI-related deepfakes, and those of us in the political realm will be at times quite intimately aware of some of the issues. It's bad enough that you have people reporting things that you didn't say as if you said it, but it's another, totally different thing to have a video of you looking like you said what you didn't say or do. Obviously, the implications are huge. I just wonder if there's any insight you can share regarding protections that individuals can have from their

likenesses being used in situations like deepfakes. I don't even know how you get a solution to that.

**Dr. Williamson:** Yes, an incredibly complex and concerning issue. One of the stakeholders on the list is an expert, actually, in that particular area, around very kind of intimate personal information. You know, that's certainly somebody, if the committee chooses, who would be able to provide a really robust explanation. But it certainly is touched upon in the Emerging Issues document around sensitive personal information and issues around consent, for sure. I hope that answers it a little bit.

**The Chair:** Member Al-Guneid, did you have any questions? Okay. Very good. Thank you.  
MLA Hunter, go ahead.

**Mr. Hunter:** Thank you, Mr. Chair. The federal government has introduced the Artificial Intelligence and Data Act, which would regulate international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements applicable across Canada for the design, development, and use of those systems and also prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests. Is there any indication as to how this would interact with existing provincial data privacy legislation such as PIPA?

**Dr. Williamson:** It's a really great question, I think more for our technical experts than for myself in terms of the Emerging Issues document, if that's all right, Mr. Chair.

**The Chair:** Yeah. That's all right.

**Ms Faulkner:** Maybe I could start. The Department of Technology and Innovation is monitoring Bill C-27 very closely on all three fronts in terms of the legislation and very much monitoring as to how it would interact not only with PIPA but also other legislation within Alberta. I cannot necessarily comment now, but I'm happy to provide a submission or additional details to the committee.

**Mr. Hunter:** I appreciate that. Thank you.

**The Chair:** Is that it? Okay.

The subcommittee on committee business met on January 29 and February 20, 2024, to review the draft list of PIPA stakeholders prepared by the Legislative Assembly Office, and a report on its activities was made available on the committee's internal website in February. In that report the subcommittee made two recommendations to the committee. The first was that the committee approve the proposed stakeholder list prepared by LAO research services with some additions from the subcommittee. The second recommendation was that the Emerging Issues document, prepared by research services, be provided to identified stakeholders when they are invited to provide written submissions to the committee.

Decision items. The committee will now look at the draft stakeholders list as recommended by the subcommittee. As noted earlier, the subcommittee reviewed the list that was prepared by the LAO and recommended that the committee accept the draft list with some additions.

Once more I'd like to ask Dr. Williamson to speak about the stakeholders list.

**Dr. Williamson:** Thank you, Mr. Chair, and thank you, members. This is my last presentation for the day. I'd like to present to the committee the stakeholder list that the subcommittee on committee

business has put forward to the committee. PIPA is a far-reaching statute, as we've seen today, and this list attempts to provide a comprehensive overview of stakeholders and those impacted by this legislation, particularly by reaching out to umbrella organizations that represent a broad range of stakeholders who are impacted by this law.

**10:40**

The list is divided into a number of different categories, including: information privacy commissioners in Canada; advocacy and privacy organizations; privacy experts; private-sector organizations such as those in business, retail, industry, finance and insurance, real estate, as well as artificial intelligence. The list also includes charities and nonprofits that are subject to the act, professional regulatory and certifying organizations subject to the act, private-sector education bodies, labour organizations, and Indigenous governing and representative organizations as well as major political parties that operate in Alberta, and this is both at the federal and provincial levels.

Just very briefly, I want to mention professional regulatory organizations. These organizations include entities such as the Alberta College of Pharmacy, the Alberta Institute of Agrologists, the Association of Professional Engineers and Geoscientists of Alberta, and the Real Estate Council of Alberta, just to name a few. So it's quite a broad range of organizations.

Just for this committee's information, research services encountered one situation with a PRO. The Alberta Boilers Safety Association is an organization that is subject to PIPA, just as an entity, and is defined as a PRO in certain legislation in Alberta such as the Fair Registration Practices Act. However, it's not completely clear that the PRO is defined in PIPA under section 1(1)(k.1). Since the law does pertain to the Alberta Boilers Safety Association, the committee may find it appropriate to contact this stakeholder regardless of its specific status as a PRO as defined by PIPA.

Thank you very much.

**The Chair:** Thank you, Dr. Williamson.

Do members have any questions relative to the stakeholders list, the draft list?

Okay. With that, I would like to thank Dr. Williamson for her work in putting these documents together and presenting them to us today.

The committee should now look to approve the stakeholders list for its review of the Personal Information Protection Act. The committee may choose to approve the draft stakeholders list as recommended by the subcommittee or with changes to it, or members may propose a different list altogether.

I'll open the floor to any discussion or motions.

**Mr. Hunter:** Mr. Chair, I'd like to move that the Standing Committee on Resource Stewardship approve the draft stakeholders list dated February 21, 2024, as distributed.

**The Chair:** Okay. Any discussion? If not, all those in favour, say aye. Any opposed, say nay. Online, if you approve, say aye. Okay. Good.

That's carried.

Stakeholders and public written submissions. Hon. members, we now have agreed upon a list of stakeholders the committee wishes to engage. During similar reviews committees have also invited written submissions from the public at large. If the committee would like, a motion could be moved to invite written submissions from stakeholders and the public. Further, as mentioned earlier, the subcommittee recommended that the Emerging Issues document be

included with the letter sent to stakeholders. The committee may consider including that in a motion.

I will now open the floor to discussion and motions on inviting written submissions as part of this review.

**Mr. Hunter:** Mr. Chair, I'd like to move that the Standing Committee on Resource Stewardship (a) invite written submissions from identified stakeholders and the public as part of the committee's review of the Personal Information Protection Act, with a submission deadline of 4:30 p.m. on May 31, 2024, and (b) direct the Legislative Assembly Office to make the Emerging Issues document, presented to the committee at today's meeting, publicly available on the Assembly's website and attach the document to the written submission invitation to identified stakeholders.

**The Chair:** Thank you very much.

Any discussion? If not, all those in favour, say aye. Any opposed, say nay. Online? Okay.

That is carried.

At our last meeting the committee had asked the LAO to prepare a communications plan to advertise for public submissions. Now that the committee has decided to seek public input in its review of the act, I'd like to ask Christina Steenbergen with LAO communications services to give an overview of the communications plan.

**Ms Steenbergen:** Thank you, Mr. Chair. Good morning, everybody. As you will have seen on the website, we have just put together a pretty brief no-cost communications plan just to create some engagement and invite submissions. Those include, obviously, posting on the committee website, so we will have a web form, and we will also have the emerging issues document on there as well. We will utilize all of the LAO's social media channels. That will include LinkedIn, Twitter, Instagram, and Facebook to bring traffic to the web form, and we'll be able to track that as well. We will have our graphics available for members to use as they see fit. We can also create an embedded JPEG invitation that you can send out to your constituents and stakeholders on your own.

As far as media relations go, we will draft a media advisory to send out probably around the first of May. I don't have a calendar in front of me for the dates. Hopefully, that will garner some engagement as well.

**The Chair:** Thank you.

Do members have any questions regarding the communications plan?

Okay. If there are no questions, I would like to thank Ms Steenbergen for presenting the plan today.

I will now open the floor to members for possible motions to approve the communication plan.

**Mr. Hunter:** Mr. Chair, I move that the Standing Committee on Resource Stewardship approve the proposed communications plan as distributed.

**The Chair:** Thank you.

Any discussion?

If not, all those in favour, say aye. Any opposed, say nay. Online? Good. Great. Okay.

That's carried.

Submission summary. Hon. members, as the committee has now provided direction on seeking written submissions, a common practice is to direct the Legislative Assembly Office to prepare a summary of submissions received. I would like to open the floor to

comments and questions or motions on this matter. Did anyone want to make a motion?

**Mr. Hunter:** Mr. Chair, I move that the Standing Committee on Resource Stewardship direct the Legislative Assembly Office to prepare a summary of the written submissions received by the committee in relation to its review of the Personal Information Protection Act.

**The Chair:** Thank you very much.

Any discussion?

Okay. All in favour, say aye. Opposed, say nay. Online? Okay. Perfect.

That's carried

Okay. Other business, request for inquiry. For the information of committee members the committee received an e-mail from Deborah Dean requesting that the committee initiate a review of Bill 2, the Alberta Pension Protection Act, as follows. As members will know, Bill 2 has received royal assent on December 7 of last year.

Are there any other issues for discussion at today's meeting? MLA.

**Mr. Schmidt:** Yeah. Thank you, Mr. Chair. If I may, for the record, just read in to *Hansard* the e-mail request that we got.

Dear Mr. Rowswell,

I am writing to you in your current role as the Chair of the Standing Committee on Resource Stewardship to ask that the committee hold a series of stakeholder and expert presentations and public input meetings to address Bill 2: Alberta Pension Protection Act.

I am aware Bill 2: Alberta Pension Protection Act has already been passed by the Legislative Assembly and came into force on December 7, 2023. And that the Assembly did not refer this bill to the Committee prior to its passage, so the Committee did not take up a public hearing on the Bill at that time. I had requested that the Standing Committee on Alberta's Economic Future take this step but the Committee Clerk, Aaron Roth, claimed it does not have a mandate in relation to the policy matters dealt within the Bill. He maintains they would most likely fall under the Ministry of Treasury Board and Finance and the Standing Committee on Resource Stewardship has a mandate in relation to policy matters under the Ministry of Treasury Board and Finance. I will agree to disagree with his assessment that the Alberta Pension Plan is outside the mandate of the Standing Committee on Alberta's Economic Future but I appreciated his referral to the Standing Committee on Resource Stewardship.

I am aware that the Standing Committee on Resource Stewardship is conducting a statutory review of the Personal Information Protection Act. It can, however, also decide to initiate an inquiry related to its mandate if it would like to. As such, I wish to make a written request to the Chair and members of the Resource Stewardship Committee, as I did with the Alberta's Economic Future Committee, to take up an inquiry related to Bill 2. I understand the Committee is busy with main estimates debate at this time . . .

Of course, that work has now passed.

. . . but a Member could choose to raise this item at a future meeting.

You may feel that the committee is not required to take these steps since the government established an independent panel of Albertans to speak with the public and get input on the possibility of moving forward with an Alberta Pension Plan. I will respectfully point out that the general consensus is that telephone town halls do not replace public input meetings and the "What We Heard" document has been tardy in its release. Further, it is the duty of members of the legislature to show transparency and accessibility in process and that can only meet

the accepted standard by making all submissions and presentations available via Assembly records, documents and transcripts, not contracted and curated reports.

I look forward to the committee agreeing to take on this responsibility. I am cc'ing all the members and the Committee Clerk in the sincere hope that it is included in a future agenda.

Thank you for your kind attention to this matter.

Regards,  
Deborah Dean

**10:50**

I agree with Ms Dean's suggestion that the committee should undertake a review of the process that the government undertook before it passed the Alberta pension plan act. Therefore, I'm moving the following motion:

the Standing Committee on Resource Stewardship undertake an inquiry into the government's policy development and consultation conducted prior to the enactment of the Alberta Pension Protection Act on the proposal set out in that act respecting a provincial pension plan.

Mr. Chair, I believe that Ms Dean has quite succinctly laid out the problems with the Alberta pension plan act, that the government has demonstrated a shocking lack of transparency or openness or even willingness to hear from the general public in person about the Alberta pension plan act and the process that the government undertook before passing that act. I think it's fair to say that many Albertans feel betrayed given that the Premier and several members of the UCP caucus during the election told Albertans that they weren't going to consider taking Alberta out of the Canada pension plan and then, lo and behold, a month later or so we find out in the minister's mandate letter that he has indeed been given a mandate by the Premier to pull Alberta out of the Canada Pension Plan act.

I think Albertans have the right to know why the government made this decision and understand how the government came to this decision even though they expressly said that they weren't going to do this during the election campaign. I think the committee owes it to Albertans to undertake this inquiry, and that's why I'm bringing forward this motion today.

**The Chair:** Thank you.

Any discussion? MLA Hunter.

**Mr. Hunter:** Well, just to correct the record, Member Schmidt had said that the Premier has given the mandate to Minister Horner to pull Alberta out. There's no such thing on any record, and he knows that. For him to continue to state this sort of thing, as the NDP have done on a regular basis, is disingenuous on his part, and he knows that.

What I will say, though, Mr. Chair, is that the Alberta pension plan act received royal assent, as you said, on December 7, 2023. I do not believe – and you can correct me if I'm wrong. The committee does not have the authority to initiate of its own accord a statutory review into legislation that has already been passed.

Now, I mean, we can continue to talk about CPP and APP. I believe that the debate is still in the public. There is still lots and lots of talk. The minister has been very clear that we are waiting for the actuaries from the federal government to provide us with more information, which I think that Albertans deserve to know. The Fair Deal Panel has stated that it's important for us to look into this, which we've done.

The NDP seem to feel that they are making some pay dirt on this, and they continue to bring it up. I don't believe that Albertans are interested in the pay dirt that the NDP are looking for. What they are interested in is getting information, which we've said we will do. I believe that that is happening. I think that for the NDP to bring

that up here once again, to grandstand on this issue in a committee that we are supposed to be working on reviewing PIPA – in fact, we have lots of time. What the member said at the beginning of this was that we wouldn't have time to be able to discuss it. We've proven that we do have time. We're not stonewalling at all. We're discussing it at this point.

But I go back to the original point, that I do not believe the committee has that ability, and I'd like to be able to know the will of the chair.

**The Chair:** Well, I'm opening this to our discussion. Is there more discussion?

**Mr. McDougall:** Well, I'd just like to agree with much of what MLA Hunter has just indicated. You know, inquiry into the government's policy development and consultation: really? I mean, this starts out with the Fair Deal Panel, that went on in 2019, and with four years of conversation before the act even came up to the floor. We've already indicated, as MLA Hunter has just said, that there's going to be further information and further consultation. This process is ongoing. It's not over yet.

We've been very clear that if there's a decision to be made, an argument to be made that Albertans may benefit from an Alberta pension plan, there will be a referendum on this question, and there will be lots of conversation and consultations and information to be considering at that time if we get to that point. Right now we're waiting for the key information, which is: what exactly is the actuarially determined number to be the portion of the fund that is attributable to Albertans if we leave? We understand that'll be coming out from the federal government in the fall of this year. We're all waiting for that information, and at that point there'll be further conversation.

You know, we don't need to have an investigation into what prior consultation was. It's a waste of our time. As MLA Hunter says, it's just the NDP trying to scaremonger and grandstand on an issue and misrepresent the reality of the situation and what's happening here, so I would suggest that we vote against this motion.

**The Chair:** Just to clarify on where I stand on it, under legislative policy committee inquiries, 52.07(2):

[The] Legislative Policy Committee may on its own initiative, or at the request of a Minister, inquire into any matter concerned with the structure, organization, operation, efficiency or service delivery of any sector of [the] public policy within its mandate.

So it is in order for the motion to be here and for us to vote on it.

**Mr. Hunter:** Thank you for that clarity, Mr. Chair.

**The Chair:** MLA Eggen, go ahead.

**Mr. Eggen:** Yes. Thank you for that clarification, Mr. Chair. You know, not only is it under our purview to choose to investigate this pension issue, but I think we do have a responsibility for the public as well. I've been in the Legislature here for a number of terms, and quite frankly I've never seen something move through the public so quickly and so intensely – right? – because underlying it all, of course, is that the pensions belong to us, all of us, and we all depend on a pension in the future or now to meet our needs.

That money is Albertans' individually, so I think that there's a very strong desire by Albertans to seek clarity on this issue. It would be, I think, quite useful for us to use this committee to help clarify the situation around pensions here in Alberta.

**The Chair:** Thank you.

Any other discussion? Go ahead.

**Mr. Schmidt:** Yeah. Thank you, Mr. Chair. I just want to remind the committee that this was an e-mail that was received from a member of the general public. This isn't an e-mail that I brought forward. This isn't a motion, this isn't a request that was initiated by me, so to suggest that we're grandstanding is a ridiculous suggestion.

But, more to the point, you know, Member Hunter has suggested that we're waiting for information. Well, this draft motion doesn't commit the committee to starting or ending the process in any particular timeline. The committee is perfectly able to set its own timeline for the investigation. We can wait for the federal government to give us a response on what they think the amount is that the province of Alberta would be entitled to if we were to withdraw from the Canada pension plan. But, more importantly, we have conflicting information from the provincial government about how much the government thinks it's entitled to if we were to withdraw from the Canada pension plan.

**11:00**

We know from briefing notes, that have been made public, to the previous Minister of Treasury Board and Finance that the amount that the civil service has estimated Alberta would be entitled to is much, much lower than what the LifeWorks report that was made public suggests. Even on that question alone I think the public deserves some clarity as to what information the provincial government is using to base its estimates on for Alberta's entitlement.

Yeah. I think, Mr. Chair, we have the responsibility, as my colleague Mr. Eggen has said, to carry out this investigation on behalf of Albertans to understand very clearly what the government intends to do with its proposal to pull Alberta out of the Canada pension plan.

**Mr. Hunter:** Just some clarity, Mr. Chair. What would we be bumping in terms of our calendar, the things that we'd be working on, in order to be able to facilitate this motion?

**The Chair:** You can't bump anything.  
Go ahead.

**Ms Robert:** Mr. Chair, thank you. The standing orders that surround an LPC's ability to self-initiate an inquiry specify that an order of the Assembly that a legislative policy committee undertake an inquiry, which the PIPA review is, shall take priority over any other inquiry. So if the committee wished to undertake a self-

initiated inquiry, it would have to be a second priority from the PIPA inquiry.

**Mr. Hunter:** Okay. All right. I think I've heard enough.

**The Chair:** Any other questions or discussion? If not, we'll go to the vote.

All those in favour of the motion, say aye. All those opposed, say nay. Online?

**Mr. Schmidt:** Mr. Chair, may we request a recorded vote?

**The Chair:** The voice vote was defeated.

Okay. The process: I'll ask the question again, and you can raise your hands, and the clerk will read your name out. Those that are in favour of the motion, raise your hands.

**Mr. Huffman:** We have hon. Mr. Schmidt and hon. Mr. Eggen.

**The Chair:** We'll get to you online there after.

All those opposed, raise your hands.

**Mr. Huffman:** We have hon. Member Armstrong-Homeniuk, hon. Mr. Hunter, Mr. van Dijken, Mr. McDougall, and Mr. Bouchard.

**The Chair:** And online. In favour?

**Ms Al-Guneid:** I'm voting in favour.

**Mr. Huffman:** Thank you, Mr. Chair. For the motion, three; against, five.

**The Chair:** Okay.

The motion is defeated.

The date of the next meeting will be at my call after the written submissions deadline has passed.

If there's nothing else for the committee's consideration, I'll call for a motion to adjourn.

**Mr. Hunter:** So moved.

**The Chair:** MLA Hunter moved that the April 25, 2024, meeting of the Standing Committee on Resource Stewardship be adjourned. All those in favour, say aye. Any opposed, say nay. Online? Okay.

Thank you, everyone. The meeting is adjourned.

[The committee adjourned at 11:04 a.m.]





