Legislative Assembly of Ontario

Assemblée législative de l'Ontario

Official Report of Debates (Hansard)

JP-54

Standing Committee on Justice Policy

Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024

1st Session
43rd Parliament

Thursday 14 November 2024

Chair: Lorne Coe
Clerk: Thushitha Kobikrishna

Journal des débats (Hansard)

JP-54

Comité permanent de la justice

Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public

1re session
43e législature

Jeudi 14 novembre 2024

Président : Lorne Coe
Greffière : Thushitha Kobikrishna

Hansard on the Internet

Hansard and other documents of the Legislative Assembly can be on your personal computer within hours after each sitting. The address is:

Le Journal des débats sur Internet

L'adresse pour faire paraître sur votre ordinateur personnel le Journal et d'autres documents de l'Assemblée législative en quelques heures seulement après la séance est :

https://www.ola.org/

Index inquiries

Reference to a cumulative index of previous issues may be obtained by calling the Hansard Reporting Service indexing staff at 416-325-7400.

Renseignements sur l'index

Adressez vos questions portant sur des numéros précédents du Journal des débats au personnel de l'index, qui vous fourniront des références aux pages dans l'index cumulatif, en composant le 416-325-7400.

House Publications and Language Services
Room 500, West Wing, Legislative Building
111 Wellesley Street West, Queen's Park
Toronto ON M7A 1A2
Telephone 416-325-7400
Published by the Legislative Assembly of Ontario

Service linguistique et des publications parlementaires
Salle 500, aile ouest, Édifice du Parlement
111, rue Wellesley ouest, Queen's Park
Toronto ON M7A 1A2
Téléphone, 416-325-7400
Publié par l'Assemblée législative de l'Ontario

ISSN 1710-9442

CONTENTS

Thursday 14 November 2024

LEGISLATIVE ASSEMBLY OF ONTARIO

ASSEMBLÉE LÉGISLATIVE DE L'ONTARIO

STANDING COMMITTEE ON JUSTICE POLICY

COMITÉ PERMANENT DE LA JUSTICE

Thursday 14 November 2024

Jeudi 14 novembre 2024

The committee met at 1000 in committee room 2.

STRENGTHENING CYBER SECURITY AND BUILDING TRUST IN THE PUBLIC SECTOR ACT, 2024

LOI DE 2024 VISANT À RENFORCER LA CYBERSÉCURITÉ ET LA CONFIANCE DANS LE SECTEUR PUBLIC

Consideration of the following bill:

Bill 194, An Act to enact the Enhancing Digital Security and Trust Act, 2024 and to make amendments to the Freedom of Information and Protection of Privacy Act respecting privacy protection measures / Projet de loi 194, Loi édictant la Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique et modifiant la Loi sur l'accès à l'information et la protection de la vie privée en ce qui concerne les mesures de protection de la vie privée.

The Chair (Mr. Lorne Coe): Good morning, everyone. I call this meeting of the Standing Committee on Justice Policy to order. We're meeting today to begin public hearings on Bill 194, An Act to enact the Enhancing Digital Security and Trust Act, 2024 and to make amendments to the Freedom of Information and Protection of Privacy Act respecting privacy protection measures.

As a reminder, the deadline for written submissions is 6 p.m. on Friday, November 15, 2024. The deadline for filing amendments to the bill is 5 p.m. on Tuesday, November 19, 2024.

Members, are there any questions before we begin our public hearings? I don't see any.

MINISTRY OF PUBLIC AND BUSINESS SERVICE DELIVERY AND PROCUREMENT

The Chair (Mr. Lorne Coe): I will call on the Honourable Todd McCarthy, Minister of Public and Business Service Delivery and Procurement, as the sponsor of the bill.

Minister, you will have up to 20 minutes for your presentation, followed by 40 minutes of questions from the members of the committee. I will give you a two-minute warning so you can sum up your presentation, sir, as you reach that point.

The questions will be divided into two rounds of 7.5 minutes for the government members, two rounds of 7.5 minutes for the official opposition members and two rounds of five minutes for the independent member of the committee.

I want to remind members to keep your mikes on—

Interjection.

The Chair (Mr. Lorne Coe): Go ahead.

I'm going to the Clerk. I can't read the Clerk's handwriting. Sorry.

The Clerk of the Committee (Ms. Thushitha Kobikrishna): Just a reminder that all mikes will be turned on by our broadcast operator and to not touch them.

The Chair (Mr. Lorne Coe): Thank you very much.

Minister, the floor is yours. Please begin.

Hon. Todd J. McCarthy: Good morning, Chair, and good morning to the members of the committee. I'm very honoured to be able to address all of you today on behalf of the Ministry of Public and Business Service Delivery and Procurement with respect to our proposed Bill 194, the Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024.

Bill 194, if passed, includes proposed amendments to the Freedom of Information and Protection of Privacy Act and would enact the Enhancing Digital Security and Trust Act, 2024.

I was pleased to see that, on October 22 of this year, the House concluded debate on second reading, and it was a robust debate on second reading of this bill. Our debate in the Legislature certainly confirmed how vital this legislation is to the people and the businesses of Ontario and to safely support the growth of our digital economy.

At work, in our homes and indeed everywhere we go, we are interacting with technology. In so many ways, it is positive. It means new ways to learn, solve problems and connect with people across the globe. It gives us access to vast amounts of information that we rely upon for business and for education—information that fuels our growing economy and adds immensely to the potential for civil society to grow and prosper. However, at the same time, we live in an increasingly digital world that presents profoundly serious risks. Cyber attacks are becoming more sophisticated and relentless, especially with the growing use of artificial intelligence. These threats pose serious risks to all levels of government, to the private sector, organizations of all types, businesses and individual Ontarians, especially our children.

As technology continues to evolve, cyber criminals are using every tool at their disposal to target vulnerable public

sector entities, including schools, hospitals and children's aid societies. Denial-of-service attacks, ransomware, phishing and cyber espionage are becoming all too common. Cyber perpetrators have absolutely no scruples and are using every tool at their disposal to target our critical sectors.

Last year, one in six Canadian businesses experienced a cyber security incident. In October 2023, cyber criminals encrypted Toronto Public Library computer systems and stole employee data, essentially shutting down services for months. Also in October 2023, a ransomware attack targeted critical systems at five southwestern Ontario hospitals, rendering them offline for weeks and costing those institutions upwards of $7.5 million to recover. A similar attack hit the Toronto Zoo in January 2024, and the city of Hamilton has spent millions of dollars to recover and rebuild its IT network after a February 2024 ransomware assault.

The Canadian Anti-Fraud Centre, in 2023, reported over 60,000 incidents of fraud, representing a total loss of $569 million, the highest on record.

According to IBM's annual Cost of a Data Breach Report, data breaches cost Canadian organizations, on average, $6.32 million per breach in 2024.

These attacks not only jeopardize sensitive information, but they also undermine public trust, national security and the health of our economy.

Bill 194, if passed, would provide the foundation to prevent, stop and mitigate cyber attacks by bolstering digital protections in our public sector organizations. As we can see by the brief examples I provided, it is imperative that we take decisive action, and take it now, to fortify our cyber defences and to safeguard our digital systems and services.

That is why introducing legislation like Bill 194, the Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024, is critical to leveraging technology to build a better, more digitally secure Ontario. In addition to fortifying cyber security in the public sector, the proposed measures would lay the foundation to strengthen protections surrounding the data and the personal information of our most precious residents: our children. Bill 194 would also introduce safeguards to ensure transparent and responsible use of artificial intelligence in the public sector.

Under Bill 194, Ontario would be one of the first jurisdictions in Canada to simultaneously regulate cyber security, children's data protections and artificial intelligence in the public sector. The intersection of these three pieces is of critical importance in the modern digital economy.

We are proud, in Ontario, to have some of the brightest minds in technological innovation and in digital security.

Bill 194 was developed in consultation with experts, academia and key public sector stakeholders, and I want to thank everyone who has contributed to date and all those who will continue to play a role, as we develop proposed regulations under the act, should it pass and receive royal assent. If the bill does pass, we would propose sector-specific requirements that could include mandatory critical cyber security incident reporting to government and tools to enhance cyber resiliency across the public sector. This bill was intentionally designed to be as nimble and dynamic as the technology and threats that will emerge. Therefore, we are committed to continuing to consult with experts and leaders across the technology and cyber security sector, ensuring that any proposed requirements reflect best practices for cyber attack prevention, cyber attack preparation and cyber attack response.

Over the course of the past several months, it has been my privilege to meet with a variety of organizations in Ontario's business and technology communities to share highlights of Bill 194 and its impacts. I've been privileged to meet with boards of trade and chambers of commerce in Brampton, Ottawa, Mississauga, Markham and Windsor. I also hosted a round table with Communitech in Kitchener, a support organization for tech start-ups, and I benefitted from meetings with the Vector Institute and the research that they provided. These sessions aimed to raise awareness about how our government is safeguarding digital privacy and data, and to gather valuable feedback as we develop potential regulations, should the bill pass.

The broad support we have received from the various stakeholders we engaged with signifies the timeliness and the importance of this work, and I am beyond proud to continue these engagements and dig deeper in the regulations phase, as we move forward together. These round tables and the engaging, open conversations that they enable are incredibly valuable as we work together to protect our fellow citizens and residents, throughout the province of Ontario in the months and years ahead.

1010

Cyber threats do not adhere to jurisdictions, to industries or to any other confinements. The best type of response is one that is coordinated and proactive—these cyber criminals will exploit any weakness in our defence system. It is vital, then, that we communicate openly across all levels of government, all regions and all sectors to ensure that there are no gaps in our fortifications against cyber threats. We are committed to engaging with partners, now and into the future, so that the people and businesses of Ontario can trust that the right protections are in place to confidently and safely participate and thrive online. By maintaining an open dialogue with partners over time, the government is committed to adapting to meet the changing needs of our people and our businesses, ensuring protections remain relevant and effective, and fostering trust in the digital landscape.

In September of this year, I had the privilege of meeting with my counterparts from across Canada who are responsible for digital trust and cyber security—this was at the federal, provincial and territorial symposium on cyber security in St. John's, Newfoundland and Labrador. We discussed three fundamental areas: cyber security, digital trust and artificial intelligence. It was a wonderful opportunity, I must say, to showcase Ontario's strong leadership on these three critical areas and to report on the decisive actions that we are taking to build digital trust. My counterparts across the country were pleased to hear

about our Bill 194 and we had many productive conversations about interprovincial alignment on cyber security. All jurisdictions agreed on the paramount need to develop strong digital trust frameworks. This will ensure that our residents are safe online. We committed to working alongside each other to build a stronger, safer and more resilient digital future for all.

Speaking to you today, Chair, about the Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024, is timely, as the Ontario public service recently completed Cyber Security Awareness Month in October. This global campaign is designed to raise awareness about the importance of protecting yourself and your sensitive data online. To kick off Cyber Security Awareness Month, our ministry was proud to host Securing Ontario's Digital Future, a symposium on cyber security for industry experts, academics and post-secondary students. It was a tremendous success, I must say, and it gave us a chance to showcase the ways in which our great province is leading the way in cyber security.

In addition to this event, each week during the month of October, our ministry released new educational materials on cyber security topics such as decoding anomalies, investigating threat terrain, protecting critical assets and future-proofing digital infrastructure. We also released new material on our K-12 Zone, an online resource for students, teachers and parents to learn about the importance of online safety. Children are at the greatest risk of harm posed by digital technology and that is why education at every stage is a principal component of our government's Cyber Security Strategy.

As you can see, our engagement and consultation for this bill has been extensive. Whether I am speaking to a fellow minister from another province or a concerned parent from a local school or a leading AI expert, the message is always the same: We need digital protections and we need them now.

Therefore, Bill 194 is built on three pillars: cyber security, data protection and the responsible and transparent use of artificial intelligence. But it is the latter pillar, artificial intelligence, that poses the most opportunity, while also coming with a significant amount of risk.

Artificial intelligence, or AI, has enormous power to increase efficiency and expand the range of products and services offered by government or business. Our legislation, if passed, would empower Ontario to leverage AI's tremendous benefits while ensuring it is used safely and responsibly across government and the public sector. It would build a strong foundation in artificial intelligence governance by setting an enterprise-wide definition of AI systems for the public sector and setting the stage for potential future regulation of AI for certain public sector organizations.

Let me be clear: Our government wholeheartedly recognizes the incredible opportunities that technologies like artificial intelligence bring, but we cannot and will not let the safety of our residents and our vital services be undermined. Through this legislation, we would support the responsible use of AI while also supporting the growth of a safe and a prosperous digital economy. By working with our partners across all sectors, we can and will achieve this goal.

As I outlined earlier, data breaches and the stealing of sensitive data is becoming all too frequent, and more often than not, these data thieves are targeting our most vulnerable residents: our children. In this world of ever-changing technological advancements, there has been no period of history where children have been subjected to the online world more than right now. Experts agree that children are at greater risks of harm posed by digital platforms, with increasing instances of privacy violations, cyberbullying and other data-related harms.

Yes, an expanding online world does provide tremendous benefits for our children, but we must recognize the unique risks they face—risks that, quite frankly, none of us ever had to face growing up. We must ensure that our children are protected from bad actors online and that their personal data is not being mined or used for harmful practices. That is why the proposed Bill 194 includes enhanced privacy safeguards to establish ways to better protect children from inappropriate data use in schools and children's aid societies, including Indigenous child and family well-being agencies. For our children, and indeed for all Ontarians, it is our duty to ensure our protections and guardrails keep pace with technological advancements. That is what we owe to our children: never accepting complacency and putting their best interests first and foremost, always.

As elected officials, every day that we do not take proactive steps to stop cyber crimes is another day that we remain open to attack. We need to act now. The bad actors responsible for cyber threats around the world need to be put on notice. Our government will not stand by and let our citizens fall prey to cyber criminals.

Ontarians put their trust in us when they chose us as their government four years ago—I should say that's two and a half years ago, actually, in 2022. I remember the date well—my first election. They trusted us to protect them and to protect their children, and that trust we take on with great seriousness and great dedication. They trust that when they provide us with personal data, whether that be at a hospital, a school or another public sector entity, that we will keep that data safe from those who may wish them harm. We simply cannot afford to be passive and wait for cyber attacks to happen. We must be proactive and stay ahead of the criminals who wish to harm our residents, our government services, our economy, our way of life and the well-being of our great province.

The bill is very crucial to Ontario's ability to safely and responsibly use innovative technologies while safeguarding against risks. The legislation, if passed, would give the people of Ontario and the businesses of Ontario critical peace of mind when interacting with their government and public sector organizations.

Chair, make no mistake about it: Our ministry consulted and engaged with cyber security experts, parents, school boards and all other stakeholders who are concerned about cyber threats, and we agree that the time is

now to act and enact the protections identified in Bill 194. We have the technology. We have the thoughtful leadership. We have the vision. We have the determination. And above all, we are on the right side of history with the values that will guide us to triumph over the cyber criminals who seek to undermine our ability to keep our residents and our critical infrastructure safe. I have no doubt that together, through this legislation, we can build a more secure and resilient digital society for generations to come.

Chair, I thank you for your time. I thank the committee members for their kind attention. Back to you for any questions through you.

The Chair (Mr. Lorne Coe): Thank you, Minister. It's always a pleasure to have you in front of this standing committee. You left one minute and 51 seconds on the clock, so I didn't need to ask you to wrap up.

1020

Going forward, before we begin our first round of questions and answers, I would like to remind the members of the committee to ask questions within the scope of the bill. That means the content of the bill. Anything outside of the bill, I will intervene and rule it out of order.

In front of the committee today for consideration, we're going to start with the official opposition, please, with MPP Glover. When you're ready, sir.

Mr. Chris Glover: Thank you, MPP McCarthy, for your remarks this morning. This is a really significant bill.

I want to start with the process of this. We have a parliamentary process in this Legislature that has been developed over hundreds of years, and a big part of that process involves committee work. Your bill specifically says that good AI policy, a good cyber security policy, is developed in a transparent way. The committee here is designed to bring transparency to the development of policy.

Last spring, your government introduced this bill, had the first reading, which meant that the opposition did not get an opportunity to speak to the bill, and then, as you said in your remarks, you had consultations all summer long. Those were private consultations. Only the Conservative Party was invited to them.

If you had had the second reading in this House, then the bill would have been before this committee, and the entire committee would have gone to the consultations, including all of the parties. With a bill as important as cyber security and AI, why did you not go through the committee process in developing the policy for this bill?

Hon. Todd J. McCarthy: Through you, Chair, to the member regarding the question: I'm happy to give the entire history and context of Bill 194. The first reality is, before first reading, when I tabled the bill on May 13, 2024, extensive consultations by my ministry officials occurred over many years. The bill—

Mr. Chris Glover: Actually—

Hon. Todd J. McCarthy: —filed at first reading—

Mr. Chris Glover: I want to reclaim my time. We're limited in my time, so I don't need the history. The question is, why did this—

The Chair (Mr. Lorne Coe): MPP Glover, I'm going to listen to the response from the minister, and I'll deal with your request to reclaim your time later. All right?

Minister, please.

Hon. Todd J. McCarthy: The proposed Bill 194 responds to findings from extensive consultations over many years held across the province with our ministry partners, the public industry, academic experts and the Information and Privacy Commissioner of Ontario. We had the cyber security expert panel's fall 2022 report. That report included recommendations on how to improve digital resilience across government and the broader public sector. We've had in place for many years a Cyber Security Centre of Excellence. We've had the cyber security learning portal in place. We've had the AI expert working group in place. And we've had many submissions since I tabled the bill for first reading.

I began second reading debate of the bill on May 28, 2024. After the adjournment for the summer recess, we continued second reading debate soon after we returned. That second reading debate, if I may say, was fulsome, with members of the opposition and government members participating. I had access to much of the thoughtful debate provided on both sides of the House.

Then the House voted to send this to committee, where we are now. We have committee days, as I understand it, today all day as well as tomorrow, November 15, and again, clause-by-clause, I understand, is planned for November 20.

Of course, as I've said, if the bill receives the support of this committee and receives the support of the House at third reading, should this committee send it for third reading, the conversations are just beginning, because the bill, of course—

Mr. Chris Glover: Point of order, Mr. Speaker.

Hon. Todd J. McCarthy: —provides for both regulations and directives. Those will only occur with further conversations across government, across the broader public sector, with input from all. This is a bill that represents a consensus-based approach, and that consensus-based approach, under my watch, will continue. This is nonpartisan and rises above politics.

The Chair (Mr. Lorne Coe): All right, Minister. Thank you for the response.

Going back to MPP Glover: next question, please.

Mr. Chris Glover: How much time do I have left on the clock?

The Chair (Mr. Lorne Coe): You have three minutes and 20 seconds.

Mr. Chris Glover: Okay, so that one question took—

The Chair (Mr. Lorne Coe): I'll let you know when there's a minute left, but you have three minutes and 15 seconds.

Mr. Chris Glover: Okay, so that first question took three minutes.

The Chair (Mr. Lorne Coe): I'm not going to rule on it right now—

Mr. Chris Glover: One of the challenges—

The Chair (Mr. Lorne Coe): Ask your question.

Mr. Chris Glover: So my point of order is, I'm going to ask the speaker to limit his responses to 30 seconds so I can get through my questions.

The Chair (Mr. Lorne Coe): I'll form that judgment. Ask your question, please.

Mr. Chris Glover: Okay.

The second question that I want to ask is: You talked about security for all public sector agencies. One of the challenges—and I've talked to a number of cyber security experts on this. They say that public sector agencies that are underfunded are targets of cyber security attacks, because they know they do not have the financial wherewithal to hire proper cyber security.

Mr. Brian Riddell: Point of order.

The Chair (Mr. Lorne Coe): I have a point of order: MPP Riddell.

Mr. Brian Riddell: We're not here to talk about funding; we're here to talk about the bill.

The Chair (Mr. Lorne Coe): I agree with MPP Riddell. Reframe your question, please.

Mr. Chris Glover: The minister mentioned a number of cyber security attacks on public sector agencies, including the Toronto Public Library, public hospitals, our zoo, the city of Hamilton. One of the reasons that we have so many cyber security attacks on our public sector agencies is that our public sector agencies are underfunded. Do you recognize that the underfunding of our public sector agencies, including our universities and hospitals, makes them and our data that they hold vulnerable to cyber security attacks?

The Chair (Mr. Lorne Coe): Minister, to the question.

Hon. Todd J. McCarthy: Through you, Chair, I thank the member for that question. The bill, if passed, is not expected to have immediate financial impacts. If anything, as the bill moves forward in a phased approach, because we're beginning with the first iteration of it, with a focus on school boards, hospitals and children's aid societies—with that phased approach, if anything, we will have cost avoidance in a significant way. I'm quite proud of that.

We've also, of course, had free access for all to the cyber security learning portal, which has been welcomed by municipalities and all members of the broader public sector as an important and regularly updated learning tool. If you see something, say something. We're all in this together and we're only as strong as our weakest link.

The Chair (Mr. Lorne Coe): There's one minute left for questions from the official opposition. MPP Glover, please.

Mr. Chris Glover: The member mentioned children at risk of online harm—as I mentioned, cyberbullying and data mining. One of the other challenges for children's mental health is the approach of social media. Nine school boards and two private schools are suing Meta, TikTok, and Snapchat for social media products that intentionally are designed for compulsive use and have rewired the way that children think, behave and learn, and educators within these boards have been left to manage the fallout.

Will this bill or the actions of this government address the mental health harms caused by social media? And why didn't you mention that in your remarks?

The Chair (Mr. Lorne Coe): You've got 12 seconds for your response.

Hon. Todd J. McCarthy: Through you, Chair, this bill leads with the protection of children, first and foremost. That includes an enterprise-wide definition of artificial intelligence. We have learned from the non-regulation of social media in the past—

The Chair (Mr. Lorne Coe): Thank you, Minister.

We move now to the government members for questions. I have MPP Bouma. Please sir, when you're ready.

Mr. Will Bouma: Thank you, Chair. Through you to the minister: Thank you for joining us today. The good folks in Brantford–Brant have displayed a growing concern regarding transparency and accountability as the government shifts towards the use of digital platforms, and that is something I hear every day. Even just yesterday, I was getting my flu shot and I asked the question, "Is there a database for everyone's health card numbers so you can see if someone has had a flu shot already?" The answer is that we're not there, but that is something that comes up all the time.

As government services continue to become increasingly digitized, many people feel concerned about accessibility and the risk of their personal information being exposed. Parents and caregivers want to guarantee that transparency will be upheld and that their voices will continue to be heard as the digital landscape expands.

I understand that this bill would strengthen the Information and Privacy Commissioner's investigative powers. Chair, through you, can the minister please describe how increasing the Information and Privacy Commissioner's investigative powers would strengthen the transparency and accountability of the government?

The Chair (Mr. Lorne Coe): Thank you, MPP Bouma, for the question.

Minister, the response, please.

Hon. Todd J. McCarthy: Thank you, Chair, and to the member from Brantford–Brant for that question. One of the schedules to the proposed bill is amendments to the Freedom of Information and Protection of Privacy Act, and the goal is to enhance the powers of the freedom of information and protection of privacy commissioner. Important features of it include the ability to make risk assessments and to act on whistle-blower protection under the act. And the act has not been updated, really, in 30 years—back when I was carrying around a brick cellphone with an antenna attached to it. So things have changed since the early 1990s, and this bill significantly updates the powers, authority and investigative ability of the Information and Privacy Commissioner, rightly so, because the protection of privacy and our personal data is so very important and is a key focus of this bill, especially for our children.

1030

I thank the member for that question, Chair.

The Chair (Mr. Lorne Coe): Thank you, Minister.

I have MPP Babikian, please, sir, when you're ready.

Mr. Aris Babikian: Through you, Chair: Minister, thank you for coming, and your staff. This proposed legislation would mandate privacy impact assessments. Our government recognizes that it is critical for us to safeguard privacy, to protect the rights of Ontarians. In turn, this would allow the citizens of Ontario to control how and where they share their personal information.

In today's digital world, we must guarantee that there is trust between citizens and government by supporting transparency and accountability when it comes to control. Minister—through you, Chair—can you tell us or elaborate on how mandating privacy impact assessments will create trust between the government of Ontario and its citizens in regard to digital privacy?

The Chair (Mr. Lorne Coe): Minister, to the question, please.

Hon. Todd J. McCarthy: Well, trust is the key—through you, Chair, to the member—and it's a very, very important point that he makes. In fact, the bill, of course, is called the Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024, as I've already indicated. And then within the bill, the other schedule is the Enhancing Digital Security and Trust Act, 2024. That schedule would enact that particular set of provisions. It's very much about trust, very much about transparency and very much about accountability.

To maintain transparency and accountability, any proposed regulations under the act, should it pass, would be published, of course, on the Ontario Regulatory Registry. The Information and Privacy Commissioner of Ontario and her office would be very much involved in a co-operative approach to ensure that the regulations are responsive to the unique needs and challenges faced by the different sectors.

The legislative framework also includes provisions for the commissioner to provide oversight and guidance on the implementation of the regulations. I, as minister responsible for the act, would be accountable, of course, to the Legislative Assembly under the principle of responsible government. That ensures our clear democratic oversight.

The Chair (Mr. Lorne Coe): I have MPP Saunderson, sir, when you're ready, please.

Mr. Brian Saunderson: Thank you, Minister and your staff, for appearing today on this important legislation. My background is partly in the municipal sector, and I know in the last eight years, one of the municipalities in my riding had a cyber attack. You spoke at length about cyber attacks both in the public and private sector, but this focuses, really, on the public sector, naming the zoo, the hospitals, a number of libraries.

These attacks can be devastating. In the instance that I'm thinking of, the municipality was effectively shut down for four weeks where they could not access records to process planning applications or GPS tracking for waste removal. It really devastated the operations of the municipality.

I'm wondering if you can explain how this legislation is going to aid our public sector in combatting and reporting these incidents so that we can monitor them and help these municipalities and public sector groups prevent them and deal with them.

The Chair (Mr. Lorne Coe): To the minister for the response. Minister, you have one minute and 24 seconds for the response.

Hon. Todd J. McCarthy: Well, the number of cyber attacks or cyber incidents number as many as $112 billion per month on the public sector and broader public sector. It's a serious risk. It's a new type of terrorism and warfare that we all have to be on guard against across the public sector and broader public sector, and in co-operation with all levels of government.

We do anticipate as a government that public sector entities will be supportive of new measures to help improve cyber resiliency and to build the safeguards for the future without requiring unnecessary regulatory burden, Chair, or without requiring unnecessary costs to organizations; in fact, we anticipate cost avoidance of great significance. Compliance with cyber security requirements is anticipated to include several benefits for all public sector entities. These include increased cyber security resilience, reduced financial impacts of cyber security attacks and less disrupted service delivery.

The Chair (Mr. Lorne Coe): Thank you, Minister, for that response.

We're back to the official opposition. Welcome, MPP Wong-Tam, back to the committee.

MPP Glover, please, to your question.

Mr. Chris Glover: Thank you, Mr. Chair. Out of respect for this committee process—I have a number of questions; I have seven minutes—I will try to limit my questions to 30 or 45 seconds. I would ask the minister to also limit his responses so that I can get through the questions that I would like to ask on behalf of the people of the province.

Let's see. The first one is transparency. You mentioned transparency several times in your statement. The word "transparency" is used once in the bill, but the term "regulation" is used 52 times. Most of the bill does not have anything of substance. All it does is provide an opportunity and the power for the ministry to make regulations behind closed doors. For people who are not familiar with it, regulations are made without public debate in the provincial Legislature, so they bypass the legislative process.

If you are developing a bill and transparency is one of the founding principles of good AI and cyber security policy, why does "transparency" appear only once in the bill and why does "regulation" appear 52 times? Why are you going to be making all the policy decisions behind closed doors?

The Chair (Mr. Lorne Coe): To the question, please.

Hon. Todd J. McCarthy: The crucial reality is, Chair, that the bill, Bill 194, acknowledges core principles, the enterprise-wide definition of artificial intelligence and an enterprise-wide definition of cyber security, and leads

with the protection of children and references the importance of protecting privacy and data for all, particularly children. So these are the core principles embedded in the act, and like any act, there's a regulation-making authority, which is particularly important in this instance because as the technology of artificial intelligence and the persistence of cyber attacks evolve so rapidly, we have to be nimble and agile. The regulation-making authority under the act, in consultation and conversation with experts, stakeholders and the Information and Privacy Commissioner, will help us be nimble and agile to keep up with and ahead of the emerging technology.

The Chair (Mr. Lorne Coe): MPP Glover, please.

Mr. Chris Glover: With that in mind, would the minister be willing to incorporate in the declaration of principles a statement about the human rights of the use of AI, appropriate uses of AI—that it would be valid and reliable, that it would be safe, that it would protect privacy, that it would be transparent and accountable, and that it would be human rights-affirming? Would you be willing to consider an amendment to the bill to incorporate a statement on human rights?

Hon. Todd J. McCarthy: Chair, through you, the bill already builds upon the Trustworthy Artificial Intelligence Framework and input from the Ontario Human Rights Commission, alongside the Information and Privacy Commissioner. So that's important because the principles that arise from that background and that are now in the bill involve these important concepts: no AI in secret; transparency; accountability; AI must always be subject to the important checks and balances of good human judgment; and risk assessment and mitigation. That is embedded as a core principle of the bill and will inform any and all regulations that would follow under the bill, should it pass.

The Chair (Mr. Lorne Coe): Thank you, Minister. New question, please, MPP Glover.

Mr. Chris Glover: Okay, so would you be willing to incorporate within that a human rights statement?

The Chair (Mr. Lorne Coe): An answer to the question, please.

Hon. Todd J. McCarthy: Chair, the bill speaks for itself. I believe we have accomplished that important balance between embracing the technology of AI and its opportunities, but also proposing safeguards, including the protection of the right to privacy for all, and in particular, our children.

The Chair (Mr. Lorne Coe): Thank you, Minister, for that response.

MPP Glover, new question, please.

Mr. Chris Glover: Yes, so we'll move on to the topic of children. Children are at great risk, and the school boards—I've mentioned this before: Nine school boards and two private schools in the province are suing social media giants for their impact on the mental health of our children. The Premier has said that he dismisses this lawsuit; he doesn't agree with this lawsuit. Yet you're talking about the potential impact of cyber security and AI on children. Will you also incorporate protections for children from social media?

1040

The Chair (Mr. Lorne Coe): Minister, to the question, please.

Hon. Todd J. McCarthy: Through you, Chair: Any litigation—of course, the member, I know, was here before me, so he would be well familiar with the principle that no parliamentarian should comment on any matter pending before the courts. But in terms of the protections for children, our government is committed to supporting measures that better protect people's privacy in today's increasingly digital world—especially our children.

With this proposed legislation, we are laying the foundation to establish Ontario as an emerging leader in setting safeguards for our children. The proposals include legislative provisions that establish regulation-making authorities to set information protections for children and for youth engaging with schools and children's aid societies. The ministry would develop and implement data protections while consulting and working closely with ministry partners, including the Ministry of Education and the Ministry of Children, Community and Social Services on sector-specific data issues.

The Chair (Mr. Lorne Coe): MPP Glover, please—through me to the minister.

Mr. Chris Glover: Our public sector agencies in this province are starving from underfunding. Eleven of our 23 public universities are running deficits this year. Our per capita health care spending is $5,000 lower. It's the lowest in Canada. It's $5,000 per person. It's 15% lower than the average of other provinces. The Financial Accountability Office projects a $21.3-billion funding shortfall in health care.

What cyber security experts have told me over and over again is that public sector agencies that are underfunded are targets for cyber security attacks. This bill—

The Chair (Mr. Lorne Coe): You have one minute left in your questions, please.

Mr. Chris Glover: Okay.

This bill asks these agencies to take on additional costs to comply with cyber security requirements. What has been suggested is that instead of just providing requirements, that the ministry and the government actually provide support, cyber security programs, to the agencies so that they can maintain the protection of our data.

Is the ministry open to providing not just requirements but actually funding and programming supports?

The Chair (Mr. Lorne Coe): You have 21 seconds, Minister, please.

Hon. Todd J. McCarthy: Chair, we've had in place the Cyber Security Operations Centre to protect all from cyber incidents and to recover from them. We have the cyber security learning portal available to all, updated regularly. We have the Cyber Security Centre of Excellence available to all. These have already been in place. With this bill, should it pass, there's no immediate financial impact—

The Chair (Mr. Lorne Coe): Thank you, Minister. That concludes the questions for the official opposition, sir.

We are now going to move to the government members. MPP Sarrazin, please, when you're ready, sir.

Mr. Stéphane Sarrazin: I think it's a really interesting subject, and having a young daughter myself, who is still at school, I know how social media plays a big role. People are really excited about artificial intelligence, and some of my constituents—I use it myself. I use ChatGPT sometimes just to look up some information. I think it's a good tool, but at the same time, I think people are worried about—they're still apprehensive towards the implementation of AI.

My question to the minister, through you, Chair, would be: Can he explain how this proposed legislation will safeguard the people of Ontario from irresponsible AI use?

The Chair (Mr. Lorne Coe): To the minister, please, to the question.

Hon. Todd J. McCarthy: To the member, there's no doubt about it that artificial intelligence is transformational technology. We have been familiar with it on our iPhones, with predictive spelling and predictive messaging—what we would call your basic artificial intelligence technology. We've moved into generative AI presently, and we're on our way to powerful AI. So this is absolutely revolutionary and transformational. As we embrace the powerful AI tools that are available to us presently, I believe that they can help us build a better province.

Ontario is introducing safeguards, however, at the same time, to ensure AI systems are used transparently, accountably and responsibly in the public sector and broader public sector. Now, as machines are increasingly relied upon to make, or assist in making, decisions, the scale and magnitude of existing risks, including bias, surveillance and threats to personal privacy, would also increase and will also increase. That's why it's important to build that trust that I spoke about earlier and to help guide safe, transparent and responsible use of AI, and that is what this legislation is designed to do.

It would, if passed, introduce an enterprise-wide definition of artificial intelligence system that is in alignment with leading jurisdictions in the world to create consistency in how AI is defined and to support AI-related initiatives across the public sector. It would create new regulation-making authorities to introduce future accountability and transparency requirements around the use of AI in the public sector and empower the ministry to set AI standards that are to be applied across the board and would be mandatory.

The Chair (Mr. Lorne Coe): MPP Triantafilopoulos, please, when you're ready.

Ms. Effie J. Triantafilopoulos: Through you, Chair, to the minister: Since our government was elected, over the past six years, Ontario has experienced unprecedented growth fuelled by our commitment to developing essential infrastructure, including new roads and highways, the first electric vehicle battery plant and the largest transit expansion in North America.

Minister, as we look to the future, the increasing integration of AI will not only streamline these infrastructure projects but also pave the way for faster and more innovative solutions in their development and management.

Can the minister elaborate on how the proposed legislation will harness the potential of AI to drive greater innovation in Ontario's infrastructure, ensuring that we remain leaders in both technology and sustainable development?

The Chair (Mr. Lorne Coe): Thank you for the question.

To the question, please, Minister.

Hon. Todd J. McCarthy: I thank the member for the question. Ontario is a leader and will continue to be a leader in so many areas, including in protecting data privacy and personal privacy and accountability with respect to the new technology of artificial intelligence and in terms of creating the ability to fortify our defences against cyber attacks. When I was joined by my deputy and my team from the ministry at the cyber security symposium for the federal, provincial and territorial ministers—and I was proud to be part of that—I could feel the respect that Ontario has across the country. I could feel that they are looking to us for leadership, and we were proud to share our Bill 194 initiatives with all other ministers, and it was well received.

Just as this government has been a leader in prioritizing vital infrastructure and investing in the green industries of the future and constructing the largest transit expansion in North America, we must also invest in the skills needed for the next generation, and to ensure that Ontario remains a Canadian and global leader for decades to come in terms of cyber security, cyber resilience and the deployment, responsibly, of AI technology.

Through the bill, my ministry and the Ministry of Economic Development, Job Creation and Trade will continue to enhance and broaden collaboration with cutting-edge experts and organizations in the field of AI, such as the Vector Institute. We recognize the Vector Institute for the dedication to its cutting-edge research and we will continue to work with and support the great work of the engineers, the researchers and the AI professionals to help accelerate the safe and responsible adoption of AI in the public sector and the broader public sector.

We've made an investment of up to $27 million in this research, and with this, the Vector Institute will broaden its support for small and medium-sized enterprises in Ontario, helping them to enhance their awareness and competitiveness through AI. But like any technology, there are incredible opportunities for the development of our civil society in a positive way, while at the same time recognizing the risks. This bill, I submit, strikes the right balance and is consistent with Ontario's leadership on so many fronts.

The Chair (Mr. Lorne Coe): I have MPP Riddell. You have one minute and seven seconds, sir.

Mr. Brian Riddell: Many of our media outlets have been increasing the number of articles published regarding cyber security breaches occurring around the world. The unfortunate reality is that cyber criminals have gotten more creative as information technology systems have

advanced. Governments now need to be ready to combat the many threats that have come with this advanced cyber crime. The government must focus on protecting the integrity and security of our digital infrastructure while sustaining the privacy and rights of citizens of Ontario. However, this burden does not fall on the government of Ontario alone. Co-operation with partners across the public sector is imperative to ensure the safety for all Ontarians.

Chair, can the minister please explain how the proposed legislation would foster an environment that ensures co-operation with the Ontario government's partners while increasing cyber resilience?

The Chair (Mr. Lorne Coe): Minister, you have three seconds, so there's not enough time for a response—

Hon. Todd J. McCarthy: Ontario is doing its part in leading in this area.

The Chair (Mr. Lorne Coe): All right.

Thank you very much, Minister—to you and your staff, for supporting you today for your presentation. That concludes your presentation for today.

The committee will now recess until 11 a.m., when our next presenter will start, that is, the Information and Privacy Commissioner of Ontario.

The committee recessed from 1051 to 1100.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

CANADIAN INSTITUTE FOR ADVANCED RESEARCH

COMPUTEK COLLEGE

The Chair (Mr. Lorne Coe): The Standing Committee on Justice Policy is back in order. We have next the Information and Privacy Commissioner of Ontario. For the record, please identify yourselves so we can get it right in Hansard.

Go ahead, Commissioner.

Ms. Patricia Kosseim: Thank you very much, Mr. Chair and members. My name is Patricia Kosseim. I'm the Information and Privacy Commissioner of Ontario. With me today are Dr. Christopher Parsons, director of technology, and Brendan Gray, legal counsel with my office.

I appreciated hearing the minister's views this morning and commend him for his bold leadership on these critical data issues of the day. Indeed, Ontario has set an ambitious goal to secure the public's confidence that their personal information will be protected in a world of digital information and AI. Bill 194 charts a path towards that laudable goal, but to truly succeed, it needs a few critical amendments.

First, for Ontarians to trust government's use of emerging technologies, there must be independent oversight to ensure these technologies are used responsibly and the risks of harm effectively mitigated. The bill currently gives the minister ultimate regulation-making authority over significant aspects of AI governance, but to be credible in the eyes of Ontarians, public institutions must be held accountable to an independent oversight body. In their 2024 statement, the G7 Data Protection and Privacy Authorities underscore the critical role of privacy commissioners in AI governance given the significant privacy and ethical implications at play. Here in Canada, Quebec's Law 25, the federal Bill C-27, Alberta's new Bill 33 and even Ontario's own white paper of 2021 all envisage explicit obligations to protect personal information collected and used as part of automated decision-making overseen by an independent privacy commissioner. Schedule 1 of Bill 194 must be amended to include this independent oversight role as it relates to the significant privacy implications of AI.

Second, AI principles and prohibitions must be embedded in the statute. For Ontarians to trust that AI technologies are being used ethically and responsibly, effective guardrails must be firmly codified in statute. This position is echoed by experts, including the Ontario Human Rights Commission, the Law Commission of Ontario, the Ontario Bar Association and Professor Teresa Scassa of the University of Ottawa. Such guardrails would ensure that AI is only used in ways that are valid, reliable, safe, privacy-protected, transparent, accountable and human rights-affirming. This is in keeping with the government's own draft Trustworthy AI Framework. Similarly, given the real risks and potential harms of AI, Bill 194 should codify in statute clear prohibitions that we all agree upon as a society should be no-go zones.

Third, there must be alignment of legal and regulatory requirements for children's digital information. Schedule 1 of Bill 194 allows for regulations to be made regarding the collection, use and disclosure of digital information of children by school boards and children's aid societies, yet there is no link between the bill and my office's existing powers to issue orders, decisions and guidance on these exact same subjects. Without amendment, the bill may inadvertently create an inconsistent and incoherent privacy regulatory regime where institutions providing services to children must comply with conflicting sets of legal requirements. Our focus should be on protecting kids, not burdening organizations with regulatory confusion and red tape. Bill 194 could be easily amended to fix this oversight.

Fourth, children's information should be deemed sensitive. The government has clearly signalled a strong commitment to protect our most vulnerable. To follow through on this commitment, Bill 194 should be amended to deem children's personal information as sensitive. This change would require institutions to apply a higher level of protection commensurate with the level of sensitivity of children's data. This special lens would apply, for example, when assessing privacy risks and implementing security safeguards for children.

Fifth, individuals must be able to complain and seek redress when something goes wrong. As drafted, only individuals notified of a privacy breach under FIPPA will have the right to file a complaint with my office. If they discover the breach through other means or if they're concerned about over-collection, use, sharing, retention,

accuracy or safeguarding of their data, they won't be able to file a complaint. Rather than advance privacy rights, Bill 194 inadvertently risks setting Ontarians back and leaving them with fewer privacy rights than other Canadians.

A critical change I recommend is to expand the grounds for individuals to bring legitimate complaints for independent investigation. Just having this option available will reassure Ontarians and preserve their trust in government.

Sixth, data minimization principles must be built in to secure Ontarians' trust in government. Bill 194 should specify that public institutions cannot collect, use or disclose more personal information than they need for legitimate and specified purposes. This data minimization principle is foundational to modern privacy laws, including Ontario's own existing privacy laws in the health and children's services sector. Bill 194, we believe, should be brought up to par so that all public institutions are held to the same basic standards.

In conclusion, Ontario has a unique opportunity to lead on the key digital issues of the day. Bill 194 is a good start, but to truly succeed, it needs these few critical and pragmatic improvements to adequately protect Ontarians and secure their trust in government. Bill 194, as amended, could lay the necessary foundation for privacy protection and responsible innovation in the digital age. Let's not miss this opportunity to solidify Ontario's leadership as we move into the digital future. Thank you.

The Chair (Mr. Lorne Coe): Thank you for your presentation.

We have the Canadian Institute for Advanced Research and Computek College joining us by Zoom. We'll wait until they join us, and then we'll listen to their presentations, and then that will be followed by questions.

Dr. Nabilah Chowdhury: Good morning, Chair and members of the committee.

The Chair (Mr. Lorne Coe): Good morning. I need your full name and your position, please, for the Hansard record.

Dr. Nabilah Chowdhury: I'm Nabilah Chowdhury, director of the pan-Canadian AI strategy at the Canadian Institute for Advanced Research, or CIFAR.

The Chair (Mr. Lorne Coe): You can start your presentation. You have six minutes.

Dr. Nabilah Chowdhury: CIFAR is a globally recognized Canadian research institution dedicated to advancing knowledge that addresses humanity's greatest challenges. We bring together over 400 researchers from around the world and are supported by the Canadian federal government, provincial governments and various partners.

Through CIFAR's pan-Canadian AI strategy, which was launched in 2017, CIFAR works to position Canada as a global leader in AI research, innovation and responsible use. CIFAR oversees initiatives such as the Canada CIFAR AI Chairs Program and the AI and society program, which provide essential support to AI research and help us better understand and navigate AI's societal impacts.

I'm here today to highlight five recommendations, on behalf of CIFAR, that we believe would help support and strengthen Bill 194.

First, we commend the Ontario government for its urgent action to address the gap in the development of digital security and AI regulations. That will ensure our public sector is equipped with transparent, accountable and secure mechanisms to support responsible AI adoption. CIFAR encourages Ontario to continue moving quickly in advancing regulatory processes that will provide the public sector with a timely and effective framework for managing AI. Speed is essential here to help Ontario remain at the forefront of AI governance and provide the public sector with the tools it needs to operate responsibly.

1110

Second, I would like to emphasize the importance of efficient implementation. We recommend that these regulations be implemented in a way that avoids creating excessive bureaucracy. By streamlining reporting and compliance requirements, the government can enable more efficient deployment of cyber security and AI protocols. This would allow public sector entities to focus on effective risk mitigation without being overwhelmed by administrative procedures. Clear and manageable regulations are key to ensuring that public sector entities can implement these important measures effectively.

Third, Ontario's approach to this legislation must be flexible. AI and digital technology are evolving at an unprecedented pace, and the legislative framework should be able to adapt to these changes. A principles-based approach would allow Ontario to respond to new developments in AI without requiring frequent amendments. This flexibility would help the government stay current, responsive and prepared for emerging challenges.

The fourth point I want to highlight is the importance of harmonizing Ontario's framework with standards established in other provinces and jurisdictions. To avoid unnecessary duplication and inefficiency, Ontario's legislation should be informed by the work already under way in other provinces and internationally. For example, CIFAR's partnerships with other provinces have provided valuable insights in collaborative frameworks that would benefit Ontario as it develops its own strategy. By harmonizing efforts, Ontario can minimize regulatory burdens, which in turn supports our world-leading tech sector.

Finally, I would like to address the need for expertise. Effective legislation must be well informed to protect the rights and privacy of Ontarians without stifling technological advancement. Ontario has access to some of the world's brightest talents in AI, including experts from CIFAR and the Vector Institute, who can provide critical insight on AI governance, safety and responsible deployment. By working with these organizations, Ontario can strengthen its own in-house expertise, helping it lead on responsible AI practices.

CIFAR is actively contributing resources to help policy-makers navigate the complexities of AI and digital security. Our AI Insights for Policymakers Program is one

of these resources, providing policy-makers with a platform to engage directly with AI experts. Through regular office hours, round tables and policy-testing exercises, this program supports informed decision-making on AI. The next session will take place on November 27, 2024, and I encourage interested policy-makers to join. Additionally, CIFAR's Destination AI course offers an accessible introductory understanding of AI's impact on society. This free online course is designed for individuals who wish to deepen their understanding of AI and its implications.

In closing, I would like to reiterate that Bill 194 is an important step towards enhancing digital security and AI governance in Ontario. CIFAR stands ready to support Ontario in implementing these measures responsibly and effectively while preserving our province's position as a leader in AI and technology. CIFAR looks forward to continued collaboration with the Ontario government to create a balanced approach that protects Ontarians' rights, safeguards their privacy and promotes the continued growth of our tech sector.

Thank you once again for this opportunity to speak today.

The Chair (Mr. Lorne Coe): Thank you very much for your presentation.

Committee members, we'll now move to a presentation by Computek College, please.

Mr. Ali Abbas Mehboob Hirji: Good morning, everybody, and thank you for this opportunity. My name is Ali Abbas Mehboob Hirji, faculty at Computek College and the incoming vice-president for technology and cyber security services.

I'll begin by stating our full support at Computek College for Bill 194. Across multiple days in September, we hosted a variety of workshops discussing the implications of Bill 194. We do not presently have any specific expertise in the field of privacy, and though we are growing that, my comments today will be specifically around cyber security and AI.

At Computek College, we have taken a very clear delineation on how we approach AI and cyber security. It is one thing, our faculty tell us, to understand how to use AI for security. It is quite the other to actually secure AI itself.

To give you a simple example, it is wonderful that we can use an AI product or a large language model, like ChatGPT, to warn staff or to train staff about a malicious email. But what if that same ChatGPT could be used to actually write a malicious email, or even write a malicious form of malware, what is also known as polymorphous malware? It is quite powerful to be able to write and synthesize documentations using an LLM, but quite the other when that same LLM can be used for data exfiltration and data leakage. From our perspective, it is important to recognize the difference between using AI for security and securing AI. We believe that, from a cyber security perspective, AI in the hands of good actors and bad actors has consequences, and Bill 194 allows us to create the necessary safeguards around this.

You've probably heard this before, and our faculty re-emphasizes, that cyber security is about people, process and technology. We believe and support Bill 194 because of three specific areas where we can help, both from a securing AI perspective as well as AI in its use for security.

Firstly, from a process perspective, Bill 194 allows us now to implement a much more robust risk management framework when it comes to AI. As some of you might be aware, the NIST, which is based out of the United States, has released a version of an RMF, a risk management framework, specific to AI. More importantly, what it does is that it creates—just as my colleague said before—certain categories of where AI can be used, cannot be used and where they are used with certain limitations and controls.

Something like the RMF framework, if we are able to execute through Bill 194, will not only allow us to have important controls, but monitoring, observability and reporting that will support better use cases for AI. More importantly, if you look at NIST's implementation and what we are seeing even across the EU, there are talks about also creating some sort of a public registry around certain AI tools so that the public is informed about the use cases and the risks involved with using certain tools. We appreciate that Bill 194 will allow us to look at implementing tools like the NIST RMF, or a localized tool created in collaboration with our partners.

Secondly, as you might already be aware, the NIST, which is a standard framework that is used quite a lot in cyber security globally, alongside ISO and many others—NIST, as of October of this year, released the ARIA sandbox. This proposes very specific methodologies to test AI tools, from red teaming, blue teaming and field testing. We find this to be a very, very important step for us to adopt such testing mechanisms.

Not only do these testing mechanisms put AI tools through a very specific standardized test, the reporting and the results are made public. And if you will, a risk register, coupled with a very clear sense of how tools were tested and approved for use, will definitely serve citizens well.

Lastly, what we enjoy about what Bill 194 will allow us to do is to also look at a future where you might even operate AI through some form of a licensing system—what is allowed to be used and what isn't, and to what extent. We see cases of this emerging out of the EU. We are, at Computek College, also looking at use cases coming out of the Middle East. We find that Bill 194 allows for robust measures, like licensing systems, around AI that will, again, assist us with building trust and the right processes around AI.

Our faculty at Computek College continues to do research in these fields. Not only did we host Bill 194 workshops, we continue to embed such topics within our curriculum and are training future generations to be equipped with the necessary tools to do the right governance, risk and compliance around AI. In the near future, we are also looking to release courses around privacy by design and security by design. We feel that we will be in a very strong position to support the necessary skill set required to append Bill 194.

1120

I thank you for your time and would like to close by quoting our CEO, Muraly Srinarayanathas, who says, "If you want to go fast, you go alone; if you want to go far, you go together." We appreciate the opportunity of going together with you on Bill 194 and look forward to assisting in whatever way we can.

Thank you very much for the opportunity.

The Chair (Mr. Lorne Coe): Thank you, sir, for your presentation.

We're now going to move into questions. They're divided into two rounds of 7.5 minutes for the government members, two rounds of 7.5 minutes for the official opposition members and two rounds of five minutes for the independent member of the committee.

I'm now going to move to the official opposition, please. Remember to keep your questions within the scope of the bill. That precludes me ruling your question out of order. Thank you very much.

You can start, please, MPP Glover.

Mr. Chris Glover: My first question will be to the Information and Privacy Commissioner. Ms. Kosseim. Thank you for being here this morning. You mentioned a number of different things. One is that the main principle that seems to be coming up, the flaw with this bill, is that everything is left to regulation. I mentioned in my previous questions that the term "transparency" is used once in the bill and the term "regulation" is used 52 times.

Why is it so important that the core principles of AI use and cyber security be incorporated into the legislation rather than be developed in regulation?

The Chair (Mr. Lorne Coe): To the question.

Ms. Patricia Kosseim: There are two tensions at play. One is you do want pragmatic flexibility for standards and regulations to evolve. In that respect, regulations play an important role for an agile, iterative regulatory regime. However, we believe that there are certain core principles that should be entrenched in statute. Everybody agrees with these core principles that I've mentioned in my remarks: that AI must be valid and reliable, safe, privacy-protective, transparent, accountable and human rights-affirming. I don't think anybody would disagree with those. Even the government itself has iterated them in its draft Trustworthy AI Framework. I think that would give enormous transparency and certainty and predictability for all players to know what are the four corners, the parameters and the guardrails that we, as a society, want to respect.

The other thing I recommend strongly is that there be certain prohibited no-go zones codified in statute. Again, that's possible by regulation, and you could always add others by regulation, but there are certain ones that we know right now we don't want to venture as a society, that are clearly harmful. The EU AI Act has incorporated prohibited no-go zones in its legislation, and we look to that as a model for some of them.

Mr. Chris Glover: What would some of those prohibited no-go zones be that you would recommend be incorporated into this legislation?

Ms. Patricia Kosseim: As examples: AI systems, for instance, that deploy subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause physical or psychological harm, and that is one example from the EU AI Act; AI systems that classify individuals or persons for the purpose of producing social scores based on their social behaviour or known, inferred or predicted personal or personality characteristics that could lead to detrimental or unfair treatment; use of AI systems that create or expand facial recognition databases through untargeted scraping of facial images; and AI systems used to assess the likelihood that a person will commit a criminal offence based solely on profiling of the individual or the person based on personality traits or characteristics.

Those are some examples.

The Chair (Mr. Lorne Coe): Thank you for that response. I have MPP Glover, please, sir.

Mr. Chris Glover: Thank you for the response. It really speaks to the science fiction nature of what AI is capable of.

The other thing that you mentioned is the protection of children. You say that this bill does not go far enough to protect the privacy rights of children, that it needs to be amended to protect children's data, and that children's data in the legislation should be deemed sensitive and be given a higher level of protection than other people's data. Can you specify exactly what you're looking for there and why?

Ms. Patricia Kosseim: There are two things that we recommend, first and foremost, with respect to children's data.

First of all, again, the bill laudably addresses children's privacy. It leaves a lot of it to regulation, and this is another area where we are concerned that there are potentially conflicting rules that will be set out by regulations by the minister or the government, and rules and orders and guidance by my office that also has oversight over exactly the same thing. So we recommend that those be reconciled in the legislation so that poor public institutions, school boards and children's aid societies don't find themselves between and betwixt conflicting rules, which would only add to regulatory confusion and red tape. That's one.

The second is with respect to schedule 2 of the bill. This is in respect to FIPPA. We recommend that the bill be amended to recognize and deem children's personal information as sensitive. This is where a lot of jurisdictions around the world are going. Children's privacy was top of mind at the Global Privacy Assembly this past year, that I attended just a couple of weeks ago.

By deeming it sensitive, there's a whole series of things that get triggered. Institutions have to consider that sensitivity when doing privacy impact assessments, for instance, and augment their protections as a result, or when developing reasonable safeguards. If we are dealing with children's personal information that is deemed sensitive, those safeguards have to be all that much more protective and secure.

It's a simple but important consequential amendment that I think aligns fully with the government's intent here, the policy objective of protecting children's privacy.

The Chair (Mr. Lorne Coe): Well, thank you for that response. MPPs Glover and Wong-Tam, you've got one minute and 40 seconds left for questioning.

Mr. Chris Glover: Okay. Let me just ask a question of Ali Abbas from Computek College.

When the Information and Privacy Commissioner was talking about embedding principles—risk assessment principles—of valid uses and risky uses of AI, or no-go zones for AI, I saw you nodding. Would you agree that those principles of AI use should be embedded in the legislation?

The Chair (Mr. Lorne Coe): To the question, sir.

Mr. Ali Abbas Mehboob Hirji: I would agree with that, and this is something that our faculty would stand by as well. It is a concept that when we teach governance risk and compliance, we talk about "by design" and not something as an afterthought. When you look at these kinds of implementations, looking at them from the standards of when AI products are being developed, not as an afterthought of what the output of the model is but what data is being ingested and how that is being used, how that data is being encrypted—this would be a necessary step, so that if it's embedded into legislation, it is something that you have to do at the get-go and not after an output is released. You do not want to be in the situation where an AI product is being put out there and is being given tabula rasa access to lots of data points, and then you start to analyze how it's used and analyze those data points with multiple algorithms as an afterthought.

It should be at the very get-go; it should be by design, and we thoroughly support that approach.

Mr. Chris Glover: Thank you so much for that response.

The Chair (Mr. Lorne Coe): You have 11 seconds, sir—

Mr. Chris Glover: I'll pass that to the government side. You can have my—

The Chair (Mr. Lorne Coe): You now have six seconds.

MPP Riddell, please. When you're ready, sir.

Mr. Brian Riddell: Thank you for your presentation. I found it quite interesting.

My question is, how can the IPC continue to work with the government to enhance strong privacy safeguards? What would your thoughts on that be?

Ms. Patricia Kosseim: Well, there are multiple ways we already do work in collaboration—

Mr. Brian Riddell: I realize that.

Ms. Patricia Kosseim: For instance, in my act, I have the authority and the power to provide comment on government programs, initiatives and legislation. I'm very happy to say that government takes us up on that and consults with our office and seeks our advice, and we provide the best advice we can to help enable laudable policy and government objectives where we can.

But when we have recommendations to make in order to make those objectives more privacy-protective or implement them in a more privacy-protective way—that's basically what we work and strive to do.

Mr. Brian Riddell: Could you elaborate on your top three that you consider the most critical recommendations?

Ms. Patricia Kosseim: Yes. In the area of artificial intelligence—well, there are more than three, but I will try to limit it to the top ones. I think recommendations 1 and 2 from our submission are related, and this is about giving a role and an independent oversight in respect of AI over schedule 1. As well, the most important, I'd say, the third, is to enable individuals to bring complaints to my office on broader grounds than currently exist—that's recommendation 18 from my submission.

1130

I don't know why but, as currently exists, the provision only allows individuals who have been notified of a breach to bring a complaint to my office, whereas many individuals may have other sources of complaint around collection or improper use or safeguarding or retention or accuracy when we talk about AI—or they may be the victim of a breach, but the institution did not advise them of it or notify them; they found out somewhere else. Why we would turn away those individuals from our door to say, "I'm sorry, you can't bring the complaint here," is really perplexing. So that would be a very simple but important expansion of those grounds to allow individuals with legitimate privacy complaints to bring them forward. Just having that availability, just having that opportunity and that possibility I think will augment Ontarians' trust in what the government is trying to do here.

Mr. Brian Riddell: Thank you for your comments.

The Chair (Mr. Lorne Coe): MPP Saunderson, please, when you're ready.

Mr. Brian Saunderson: Thank you to the presenters today for their input on this important legislation.

My question is for Ms. Chowdhury and Mr. Hirji—I hope I've said those names correctly. I taught at Georgian College for a while—that was a long time ago—and back in the day, the kids had to put their essays through a machine or a program that would check to make sure there was no plagiarism. Now, with the development of ChatGPT and other mechanisms, that whole world has changed.

My question for each of you is, what would you identify as the high-risk AI uses that are going to become prevalent? How, in a regulatory framework, do we effectively tackle those while allowing for innovation and allowing for the evolution of that innovation? It seems to me that we've got a moving target here. How do we pin it down?

The Chair (Mr. Lorne Coe): Thank you, MPP Saunderson.

To the question, please.

Mr. Brian Saunderson: I'll start with Mr. Hirji, please.

Mr. Ali Abbas Mehboob Hirji: I'll keep this brief, and I will say that for us at Computek College, one of the most

intense threats that we see is the weaponization of AI and the hands by which some of these tools have been used.

I'll give you an example. When we teach ethical hacking and security, we use a lot of open source—these are tools that you can use that are accessible without pay attached to it. You could go online today and download some of these tools and do active scanning, or what we call reconnaissance, on an environment to see what devices are connected. But before we even make the students do any of these activities or even learn about it, they do sign a waiver and go through a security training course to understand their responsibilities when using these tools. These are specialized tools today. If you look at your LLM models that are out there today, these LLM models can actually write for you malicious code and malicious malware, which can be used by a completely lay actor and deployed into an environment—someone who has very limited technical skills. So for us, when we look at the biggest threat, 100% we look at LLMs and we look at social engineering techniques as the biggest threats that can be used and weaponized against citizens of Ontario.

Mr. Brian Saunderson: Thank you. And Ms. Chowdhury?

Dr. Nabilah Chowdhury: I'll just add on to Ali's sentiments. It aligns with what CIFAR is saying, that we just must be able to adapt. Having principles-based legislation and having the legislation move just as fast as the technology will be important in being effective to addressing these threats.

Mr. Brian Saunderson: Thank you very much. Those are my questions.

The Chair (Mr. Lorne Coe): Thank you, MPP Saunderson.

You have one minute and 14 seconds for the government. Further questions, please? MPP Babikian.

Mr. Aris Babikian: My question is to the privacy commissioner. You have recommended expanding the circumstances where it can share information to carry out its mandate—I mean the IPC. Can you explain the IPC's rationale for this recommendation and how it would strengthen the IPC's ability to effectively oversee privacy protections under the new legislation?

Ms. Patricia Kosseim: Yes, this is an important provision that I understand will be elaborated by way of regulation. But it is critical in order for us to be able to fulfill our mandate and in order to fulfill the objectives of the bill, which is basically to build Ontarians' trust in digital information and artificial intelligence used by public institutions.

Let me give you a concrete example. Through this legislation, in schedule 2, there will be mandatory breach notifications, so institutions must notify my office if there are privacy breaches—

The Chair (Mr. Lorne Coe): Excuse me, Commissioner. That concludes the time that you have available to answer that question.

We're now going to turn to the official opposition. MPP Wong-Tam, please, when you're ready.

MPP Kristyn Wong-Tam: Thank you to all the speakers who have appeared before the committee today for your presentations.

My question to you, Commissioner, is that—you've put before this committee a fairly lengthy submission. I want to state that it's 37 pages long, with 28 specific recommendations on how to strengthen and improve this act. And your top line—I wouldn't say that it's the only one; there are several top lines, but I think that a very important one that jumps out to me is the absence of clarity on the purpose of this bill, specifically around your recommendation that the minister put forward substantive statutory rules governing the collection, use, disclosure and retention of all this data and use of AI.

Given your role as commissioner—you're here to enforce the privacy and access rules of Ontario—how much consultation was there with your office prior to the drafting of this bill, the introduction of this bill?

The Chair (Mr. Lorne Coe): To the question, please.

Ms. Patricia Kosseim: I would say there was significant consultation in the development of the bill, and it was a very collaborative, open process. But many of our recommendations, of course, were not necessarily taken up, and that's why I'm here today to bring those recommendations forward.

MPP Kristyn Wong-Tam: I see. Thank you.

And because your recommendations via submission are very thorough—each line has a very clear rationale on why it needs to be included, including the specific language that you would use to amend the act—I'm just curious to know whether or not the minister or the ministry staff provided any explanation why these 28 specific drafted amendments were not included.

Ms. Patricia Kosseim: In some cases, yes; in some cases, no.

MPP Kristyn Wong-Tam: Can you give us an example of a reason why it would not be included?

Ms. Patricia Kosseim: An example might be, for instance, difference of perspective on whether or not what we were recommending was within the scope of the bill.

MPP Kristyn Wong-Tam: I see. And you are the top officer in the province when it comes to safeguarding privacy and access to information for Ontarians. Is that not correct?

Ms. Patricia Kosseim: I'm an independent office of this Legislature with a mandate to oversee those two fundamental principles, yes.

MPP Kristyn Wong-Tam: Yet the bill does not have any instrument that creates independent oversight on how the act would be implemented, enacted and ultimately enforced. Is that correct?

Ms. Patricia Kosseim: In part. Schedule 2 does reinforce my role in overseeing privacy investigations and complaints, though limited, as I mentioned. Schedule 1, however, makes no reference to my office at all.

MPP Kristyn Wong-Tam: Because the reference to your office is rather limited, even on how the grounds of complaints would be brought forward—only via public disclosure or public notification—individual Ontarians are

restricted from having access to your office via complaints if they want to initiate something on their own. Is that correct?

Ms. Patricia Kosseim: By the scope clause of the provision that allows individuals to bring complaints to my office, it is one of the most narrow clauses that I have seen.

1140

MPP Kristyn Wong-Tam: Thank you. Because the role is so restricted, we know that, oftentimes in Ontario, what brings to light problems are those who are seeing it first-hand, those who may be working in the ministries. We have whistle-blower protection to allow bureaucrats and those who work in the ministry to shine a light on the wrongdoing or a matter that requires full public transparency and accountability. There are no whistle-blower protections, as it exists, in this act. Is that correct, or is it touched upon but just not enough?

Ms. Patricia Kosseim: I think it's touched upon, but not enough. I'll ask Brendan to fully answer the question, Mr. Chair, if that's okay.

The Chair (Mr. Lorne Coe): Yes, please. Thank you. I need his name and his title.

Mr. Brendan Gray: My name is Brendan Gray and I'm legal counsel at the IPC.

In the IPC submission, there are some additions to the whistle-blower protection in schedule 2, so there, it needs to be added to include particular protections for whistle-blowers, and then we recommend that an entire whistle-blower clause be added to schedule 1.

MPP Kristyn Wong-Tam: Thank you very much. That is very helpful.

May I ask about the process that the minister outlined in his submission that he's undertaking? A lot of the discretion around regulations is going to be done in private. For a shorthand, to explain to folks who are watching what regulations do: We are debating this bill publicly, but the details, the meat of the bill, are going to be done in private. We will not have a chance to consider it; we won't have a chance to provide feedback.

It is your opinion that when it comes to the principles of how we manage AI—what is permitted, what's not permitted—it should be done in public. Is that correct?

The Chair (Mr. Lorne Coe): Commissioner, you have one minute and 30 seconds for your response.

Ms. Patricia Kosseim: Thank you for letting me know.

I think there are multiple layers to answer that question. First, there is no doubt that the legislative-making process is more transparent, generally, than the regulation-making process. But even the regulation-making process—and there is room for regulation; it's important to have agile regulations in some respects. But that too can be a much more transparent process. Many of our recommendations are actually about making that regulation-making process much more transparent.

I would say that regulation can only exist to the extent that it can hang its footing into the law. If there are core provisions that are not in the law, then the regulations cannot stand. We cannot talk about regulations unless there is a legislative footing in the statute. That's why we are making some key recommendations to ensure that at least that footing is there, so then we can go on and elaborate and work together on regulations.

The Chair (Mr. Lorne Coe): Thank you.

You have 25 seconds, MPP Wong-Tam. I would suggest you might want to—well, you won't be posing a question, will you, as it's 20 seconds.

MPP Kristyn Wong-Tam: Well, now I have 11 seconds.

The Chair (Mr. Lorne Coe): There won't be time for a response. Okay, thank you.

MPP Kristyn Wong-Tam: Six seconds.

The Chair (Mr. Lorne Coe): I'm going to the government members, please. MPP Triantafilopoulos, please.

Ms. Effie J. Triantafilopoulos: Thank you so much for a very substantive presentation today, Commissioner. I have a couple of questions. One is, how do these proposed measures align with your recommendations to enhance data protection and service delivery in Ontario? If you could be more specific on that.

Ms. Patricia Kosseim: You mean the bill in general?

Ms. Effie J. Triantafilopoulos: Yes.

Ms. Patricia Kosseim: First of all, I commend the government for putting their finger on the most important data issues of the day: cyber security, AI, children and data protection. There is no question this is significant. Ontario has a huge opportunity for leadership. There are differences in how we would go about doing that—many of which we support in the bill, of course. But my recommendations are where it can be improved, either slightly improved, or, as I said, trying to really focus in on those key critical amendments—few but important—that will really make a game-changing impact in terms of what we all want, which is better data protection for Ontarians.

Ms. Effie J. Triantafilopoulos: Thank you for clarifying that as well.

You've advocated for a risk-based approach to AI regulation. Can you elaborate on the types of high-risk AI uses that you believe should be the focus of government regulatory efforts under Bill 194? How would this help protect Ontarians while enabling responsible innovation as well?

Ms. Patricia Kosseim: I will be referring this to my colleague Dr. Chris Parsons. I'll just introduce by way of saying that regulations and laws around the world have introduced risk-based approaches—either harm-based or risk-based—to ensure that the regulation and legislation governing AI is proportionate to the level of risk or harm, which is what you want in an economy and space where you want to promote innovation. We are supportive of this proportionate approach, commensurate with risk or potential harm.

Could you give us some examples, please?

The Chair (Mr. Lorne Coe): Dr. Parsons, please.

Dr. Christopher Parsons: Thank you for the question. The commissioner has outlined a number of no-go zones. Public scraping from cameras to develop facial recognition systems, we think, is so high-risk that it should simply be barred by definition.

We also have identified a series of principles, which the commissioner has noted, as a way of setting the baseline

for how all technology should be designed. We expect our technologies to be safe, human rights-affirming, transparent, accountable, privacy-protective, valid and reliable—which just means they work. Once we've got that done, we can go through and start considering when artificial intelligence technologies may have significant impacts on individuals' lives and there is also a limited ability to reverse that situation without causing undue harm.

In the criminal justice system, as an example, using an AI system to profile individuals for bail: We've seen in numerous studies to date that this has led to individuals being incarcerated based on scores, and those scores have been problematic, to be generous, in the way they have been developed. Similarly, with child welfare systems and the allocation of benefits, when benefits are cut off from those who are most vulnerable in our society, it can have devastating consequences, and they may not be able to recover.

So I think it's imperative when we adopt a risk-based approach to contemplate what are the high-risk situations where we can harm Ontarians, which is none of our intent, and ensure that we avoid those, while simultaneously recognizing there may be lower-risk situations where they may have lower consequences and be quickly reversible. Those might be easier systems to deploy more rapidly.

Ms. Effie J. Triantafilopoulos: Thank you.

The Chair (Mr. Lorne Coe): New question, please, for the government. You have three minutes and 18 seconds remaining.

MPP Babikian, please.

Mr. Aris Babikian: Chair, through you to the commissioner: This technology is evolving—AI, cyber security etc. There are many players, many factors—local, international, government, NGOs, underground organizations; they are trying to take advantage of it. In this bill, we are addressing some of these issues. This is a first on a provincial level, that a provincial government has started thinking about it, opened dialogue, consulted and now legislated a bill.

Don't you agree with me that we need to give government an opportunity, since this is evolving and we don't know what we are going to face down the road? Wouldn't you agree that we should give the government the opportunity to be flexible to address the future issues that we're going to face in this industry? Because we cannot foresee the future, no one can tell what is going to happen or how this technology is going to evolve or be used.

I just want your comment on this issue—that at least this is a first good step on behalf of the government of Ontario.

The Chair (Mr. Lorne Coe): Commissioner, you have one minute and 56 seconds for your response, please.

Ms. Patricia Kosseim: Thank you for the question. There's no issue with the advantage of evolving the legislation and rules through regulation. As I mentioned before, it's a rapidly evolving space of great innovation and change. Regulations over time will help, I think, adapt in an iterative and agile way to a changing landscape.

There are, however, as I mentioned before, principles and guardrails that must be entrenched in statute. I cannot imagine a day, and hopefully neither can you, where we don't want our AI to be transparent, accountable, human rights-affirming, privacy-protective, valid and safe for our Ontarians. Those principles are non-changing. Those are foundational principles, similar to no-go zones. I can't imagine a situation where we would want to harm Ontarians in the ways that my colleague described, so those are the things we are hoping will be entrenched.

The government does have an opportunity. It has a great opportunity with this bill, I would venture to say, in the days ahead, to make some government amendments—or this committee has a chance to make some amendments that will make this bill give Ontario a real global leadership opportunity to regulate this space and be an envy of the world in how you do it.

The Chair (Mr. Lorne Coe): Thank you, Commissioner. That was perfect; just three seconds left for your presentation. Very good.

That concludes our questions and answers of our delegation today. The committee will now recess until 1 o'clock today. Please be on time.

The committee recessed from 1151 to 1300.

The Chair (Mr. Lorne Coe): Good afternoon, everyone. The committee will resume public hearings on Bill 194, An Act to enact the Enhancing Digital Security and Trust Act, 2024 and to make amendments to the Freedom of Information and Protection of Privacy Act respecting privacy protection measures.

As a reminder, the remainder of our presenters today have been scheduled in groups of three for each one-hour time slot. Each presenter will have seven minutes for their presentation, and after we've heard from all three presenters, the remaining 39 minutes of the time slot will be for questions from members of the committee. The time for questions will be broken down into two rounds of 7.5 minutes for the government members, two rounds of 7.5 minutes for the official opposition and two rounds of 4.5 minutes for the independent member.

Not to be repetitive, but please remember to keep your questions, committee members, within the scope of the bill. That will preclude me interrupting you and asking you to re-put your question or to ask for a new question because the original question was not within the scope of the committee. I would prefer not to be able to do that, so let's work as we did this morning. We had a lot of success together. Moving forward, let's continue in that vein, please, okay?

VECTOR INSTITUTE
MR. FARIBORZ LESANI
TECHNATION

The Chair (Mr. Lorne Coe): I will now call on the Vector Institute, Technation and Fariborz Lesani—and I apologize if I mispronounce that going forward.

You can start your presentation, please. You will have seven minutes for your presentation. Please state your name for Hansard and you may begin. Remember, you only have seven minutes, because I'll stop you if you go over seven minutes, and you don't want that, okay? Thanks very much.

Please begin—your name first.

Ms. Roxana Sultan: Thank you, Mr. Chair, and members of the committee. My name is Roxana Sultan. I'm the chief data officer and the vice-president for health at the Vector Institute for Artificial Intelligence. I'm pleased to be here to discuss Bill 194, the Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024.

The Vector Institute is an independent, not-for-profit organization dedicated to advancing AI innovation and adoption to drive economic growth and to improve the lives of Canadians. Supported by government, industry and academia, the Vector Institute plays a vital role in growing Ontario's AI ecosystem. We are one of three Canadian AI institutes established under the Pan-Canadian AI Strategy, and we are home to over 850 AI experts and have a talent pipeline of over 1,700 students who are leading the way in shaping the future of AI. Our extensive network includes partnerships with over 30 large industry sponsors, more than 300 Ontario-based start-ups and scale-ups, and more than 60 hospitals and life sciences institutions, which together create a thriving AI ecosystem in the province. This ecosystem is not just an engine for economic growth, but a dynamic force that drives solutions across sectors like health, financial services, manufacturing and more.

At Vector, we believe in AI's potential, and we also believe that this potential must go hand in hand with trust, safety and ethical use. Our published AI trust and safety principles reflect our commitment to these values. AI should benefit people and the planet, uphold democratic values, protect privacy and be robust and secure. These principles are not just words; they are the foundational aspects of our work and guide us to develop AI with accountability and transparency. We recognize that if AI is to be truly transformative, it must be developed and used in a way that the public can trust.

Globally, we're seeing unprecedented growth in AI, with governments worldwide ramping up their investments and capabilities, and the private sector investments surging. For Ontario to remain competitive, we need to continue investing in our AI ecosystem, and much of our work at Vector is focused on building Ontario's AI capabilities so that we can meet this challenge. Our Smart Health initiative and the pan-Canadian AI compute environment, or PAICE, are excellent examples of government-supported programs that are driving efficiencies, building AI capacity and fostering innovation across the province.

Through the Smart Health initiative, for example, we've been driving measurable impact by developing and deploying AI-enabled solutions in Ontario hospitals that are improving patient outcomes, increasing efficiency and reducing caregiver stress. Our implementation of the PAICE initiative is helping build the infrastructure that we need to support advanced AI discovery in Ontario, keeping us competitive on the global stage. These initiatives demonstrate the value of partnerships between government, research and industry, and are concrete steps towards building a strong and sustainable AI ecosystem in Ontario.

While the growth of AI is promising, there's an equally urgent need for guardrails to ensure that AI is used ethically and transparently. Establishing clear legislation and policies to provide ethical standards to guide AI practices is essential to building public trust and ensuring that AI serves the best interests of everyone in Ontario. That's why Vector supports and commends the Ontario government's development of Bill 194. This bill addresses critical areas like AI, cyber security, child protection, and privacy, all of which are essential to consider in today's technology-driven world. By tackling these issues, Ontario is showing leadership and foresight in setting a foundation for AI safety. We applaud the government for taking these proactive steps to protect Ontarians while fostering a responsible approach to AI innovation.

We also believe that there's an opportunity to build on this framework to make it as comprehensive and practical as possible as we move forward. One area for further development is the enhanced authority proposed for the Information and Privacy Commissioner, or the IPC. For instance, the proposed amendments would allow the IPC to conduct privacy investigations and administer compliance orders across public institutions, which is crucial for protecting personal data. That being said, we need to ensure that this doesn't inadvertently create a chilling effect, especially regarding the sharing of de-identified health data for AI discovery and innovation. A balanced approach will help maintain data privacy without impeding critical health innovation. One way to achieve such a balance would be for the IPC to collaborate with the Vector Institute to ensure that the definitions of appropriate data use enable and not hinder legitimate AI research.

Vector is also well positioned to support the development and implementation of frameworks that strike a balance between governance and innovation. With our expertise in privacy-enhancing technologies and data governance, we can help shape a practical approach that supports public safety while encouraging responsible AI development. Currently, the AI provisions in the bill largely serve as enabling structures, meaning that much of the practical impact will depend on future regulations. This will allow us to work together to develop a framework that achieves real, actionable impact while ensuring that Ontario's AI advancement continues.

The bill's transparency and accountability requirements are also a crucial step forward, including provisions for public notification when AI systems are in use and ensuring that there's always a channel for human review in AI-driven decision-making. These measures help address concerns about AI bias and safety, which are essential for building public trust. To enable these goals, Vector could serve as an independent validator for AI

models in sectors like health care, leveraging our frameworks that we've developed for evaluating AI safety.

The Chair (Mr. Lorne Coe): You have one minute left.

Ms. Roxana Sultan: Given that many public institutions face a flood of AI solutions from various vendors, a trusted evaluation process led by Vector could guide these organizations in selecting AI tools responsibly and effectively. We envision a potential partnership with the government where public funds would be allocated only to AI solutions that have undergone Vector's assessment. This approach would operationalize Ontario's trustworthy AI framework and establish evaluation standards for publicly funded AI initiatives.

In closing, we appreciate the positive steps the government has taken to address AI safety and accountability and look forward to working with all of you to ensure this legislation continues to strengthen AI ecosystems in Ontario, balancing innovation with ethical standards that protect and serve the public.

I'll be pleased to take your questions.

The Chair (Mr. Lorne Coe): Thank you. You did very well; you had nine seconds left.

We have someone ready to make a delegation via Zoom. Can we bring up our next presenter, please?

Fariborz Lesani—good afternoon, sir. How are you?

Mr. Fariborz Lesani: Good afternoon. Good. Thank you.

The Chair (Mr. Lorne Coe): You have seven minutes for your presentation. As you probably heard me with the last presenter, I will end your presentation if you go over. Everyone has the same time limit, so I'm not being uneven in that. Please start your presentation, sir.

Mr. Fariborz Lesani: My name is Fariborz Lesani. I'm a technology consultant in Toronto with a focus on tech-for-good projects. Thanks for this opportunity.

Today, we often treat AI as just another branch of digital technology. We talk about cyber security but we rarely mention AI security. We focus on cyber attacks but not AI-driven threats. We teach digital literacy but not AI literacy.

AI represents an entirely new paradigm. Its rate of progress is outpacing what we saw with digital technology. Today, we have cyber-specific centres of excellence, protection methods and training hubs. But addressing AI through a traditional cyber lens is like trying to drive forward while looking in the rear-view mirror.

1310

Consider this: Applied AI has been around for decades, but AI that directly impacts the public is just two years old, introduced by tools like ChatGPT. Yet, we have seen 10-year-olds already using it, and using it widely. This adoption is happening faster and at a younger age than we ever saw with digital or social media. And yet, AI literacy doesn't feature in our curriculum. Teachers haven't been trained in it, and public awareness is minimal.

Just today, OpenAI released Operator, an AI agent capable of taking control of a user's computer by choice and performing tasks in the physical world.

AI has moved beyond the digital. It's breaking out of our screens and into our physical lives, making traditional cyber approaches insufficient. While no one can predict the future, our experience with media and digital literacy gives us valuable insights. We know that a lack of foundational understanding leads to unintended consequences, from misinformation to security risks.

AI's rapid evolution demands proactive adoption if you want to keep pace, but AI literacy for responsible AI cannot fall behind. This bill makes an excellent start and covers essential AI-related security concerns, but it still primarily reflects a digital-first mindset. There's a need for a new framework that includes proactive AI literacy.

My recommendations focus on establishing public awareness and resilience as both the first and last line of defence. I'm going to go through my list of recommendations.

Introduction of AI literacy and awareness programs: Introduce AI literacy, not just in technical terms, but focusing on the social impact. This should start with educators and be integrated into K-12 curricula.

AI literacy for public service employees: Equip public service staff with the understanding needed to recognize AI's impact on their work and on the people they serve.

Economic and social importance of an AI-driven future: While not for this bill specifically, AI literacy should include understanding the future of work and socio-economic security in an AI-first world.

My own 12-year-old already uses generative AI tools, yet has never received any formal training on AI risks or best practices. This technology may be young, but its impact is scaling faster than the last two decades of digital progress.

We were 20 years late implementing digital literacy. We are already late for AI literacy. It's time to decide how we will incorporate AI literacy into our education system and public service sectors quickly and decisively. Thank you.

The Chair (Mr. Lorne Coe): Thank you, sir, for your presentation.

Our next presenters are from Technation. Before you start, I need both of your names for Hansard, please.

Ms. Angela Mondou: Angela Mondou.

Mr. Prateek Sureka: Prateek Sureka.

The Chair (Mr. Lorne Coe): Thank you. Please begin.

Ms. Angela Mondou: We're pleased to speak to Bill 194, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024, and its significance to Ontario's growing tech sector.

As Canada's leading tech association, Technation unites industry, government and communities to drive economic prosperity and global competitiveness through technology adoption. For over 60 years, we've represented Canada's $242 billion in the ICT sector, including 70% of our small-medium members and innovators, many of whom are based in Ontario. These members drive technology growth, global competitiveness, and contribute $48.3 billion to Ontario's GDP, employing over 408,000 workers.

At Technation, we champion digital innovation, shape technology policy, and advance technology adoption and prosperity through a number of initiatives, including our AI4Canada national summit, accelerating responsible AI adoption across the nation, but also a call to action for government-industry collaboration on AI policies. We also advocate for procurement, modernization and agile procurement, fostering a thriving economy for technology firms, and driving a national security agenda with our cyber security task force, highlighting industry's role in safeguarding Canada.

As Minister Vic Fedeli recently said, innovation thrives in Ontario. With over 25,000 tech companies, Ontario's tech sector is one of the largest in North America. I had the opportunity to work for two of these superstars, both at Nortel Networks and BlackBerry—all of these companies contributing billions annually to the gross domestic product.

We commend Ontario's leadership in cyber security and AI, and we believe it is crucial for Ontario to lead in establishing a framework that takes cyber security seriously and seizes the opportunities AI offers while managing its risks.

This bill, and its regulations to follow, will set the stage for Ontario's public servants to leverage AI to make better, faster decisions, and increase service efficiency for Ontarians. With AI's potential to add $100 billion to Canadian small-medium enterprise productivity by 2030, Ontario is setting a powerful example for the rest of Canada by driving AI adoption and supporting responsible AI use in government.

In addition, to capture AI's potential, Ontario must deliver policies that attract AI investment, create jobs and encourage public sector adoption.

We at Technation have appreciated the opportunity to contribute to government's early consultations on Bill 194. We also recommend ongoing consultation to co-develop industry standards for AI fairness, privacy and non-discrimination. We would recommend and collaborate on best practices from sensitive sectors like health care to ensure data protection, privacy and anonymity, ensuring public trust. Technation supports a light-touch regulatory approach that encourages AI adoption while safeguarding citizen rights and building trust.

I want to note that increasing public trust in AI is essential. Currently, trust in AI in Canada is 23% lower than the global average due to concerns, lack of education and unfamiliarity. We recommend a targeted public education campaign to build understanding, which would involve incorporating AI education and its benefits through ethical use into the provincial curriculum. This approach will strengthen public trust and appreciation for AI's role in government services, but also for business and our citizens.

Technation also plays a significant role in tech and cyber security skills development through our Career Ready Program, which connects students across Canada with tech sector jobs. In Ontario, we've invested $18 million and created 3,880 tech positions as part of a student's education, setting them up for success as tech- and AI-ready employees, but also setting up Ontario industry.

Through Supply Ontario, government aims to simplify process and encourage companies to do business with Ontario. The tech sector and AI technology should play an important role in this space, as AI holds tremendous potential to enhance public service productivity, especially in complex procurement process. Governments are now transforming to agile procurement process to better align with the ongoing and accelerating transformation of technologies.

On behalf of Ontario's tech sector, I emphasize our commitment to partnering with Ontario, and I want everyone at Queen's Park and in the surrounding government buildings to know that.

The recently launched Building Ontario Businesses Initiative, or BOBI, is a positive step in reducing barriers to public procurement, and a targeted approach with the tech sector is also needed. Automating vendor management, centralizing process, using predictive analytics, incorporating sustainability metrics are just some of the ways Ontario can improve procurement for tech companies.

Technation's agile procurement platform, the government digital marketplace, has seen success with Shared Services Canada by connecting government procurement leaders with Ontario's technology innovators while increasing small-medium enterprise access and visibility to government opportunities. We recommend piloting this approach in Ontario to create more opportunities for Ontario tech innovators, scale-ups and minority-led business.

1320

Given escalating global cyber threats, our cyber security task force advocated for shared cyber security services to support small municipalities and small and medium enterprises. Technation has recommended a collaborative approach—a public-private sector approach—to help Ontario counter these threats effectively as well.

In closing, I want to thank the committee for inviting us to speak on Bill 194 and the government of Ontario for including Technation in this conversation. Continued partnership will be essential to building public trust in AI and supporting Ontario's digital leadership. Technation sincerely looks forward to working with the government to enhance data protection, privacy, service delivery and AI adoption across the province.

The Chair (Mr. Lorne Coe): Thank you very much for all of your presentations.

We're now going to turn to the official opposition for questions, as I indicated in my introductory statement when we came back. I have MPP Glover, please, sir, when you're ready.

Mr. Chris Glover: Thank you all for coming here today and for your presentations.

I heard a couple of common themes, and I'll pick up on those first. Ari, you were suggesting the need for education, and Angela, you were also suggesting the need for

education to address the lack of trust in AI in the Canadian population.

Angela, I'll ask you first: Why is this so essential?

Ms. Angela Mondou: Because trust in an emerging technology is the foundation for someone to adopt. If we're looking at Canadians and citizens in Ontario and across the nation to be comfortable and understand what AI is all about, how it's going to impact their work—will it impact my actual job—having trust in the technology, first and foremost, is critical.

Mr. Chris Glover: Okay.

One of the recommendations that was made by the Information and Privacy Commissioner was to incorporate a declaration of principles into this bill that would include that AI should be used in a manner that is valid and reliable, safe; protects privacy; is transparent, accountable and human rights-affirming.

Would you agree with that amendment?

Ms. Angela Mondou: Yes.

Mr. Chris Glover: Yes? Okay.

Ari, I'll ask you as well: Would you support that amendment to the bill to increase trust among the public?

Mr. Fariborz Lesani: Yes, for sure.

Mr. Chris Glover: Yes? Okay.

And, sorry, I lost your name—Roxana.

Ms. Roxana Sultan: It's going to be yes as well.

Mr. Chris Glover: So everybody is in agreement on that one.

The other thing that was a recommendation from the Information and Privacy Commissioner was to protect the privacy of children. She said that we need to amend the bill to protect children's data, because children's data should be deemed sensitive and needs a higher level of protection than for adults.

I'll go around the table again. Roxana, would you agree with that?

Ms. Roxana Sultan: My sense from the existing legislation is that there is significant recognition of the unique nature of protection for children, so I'm not sure that anything specific is needed to amend, but if we want to re-emphasize that, I don't see any harm in doing so.

Mr. Chris Glover: Okay. Thank you. Angela?

Ms. Angela Mondou: I'll have my colleague Prateek answer that question.

Mr. Prateek Sureka: Bill 194 includes a provision specifically aimed at protecting data of individuals under 18 years of age, with a focus on sectors like children's aid societies and schools—some pretty good measures, which ensures the vulnerable population is protected. So the bill already has a number of provisions that take care of children—

Mr. Chris Glover: So this bill is focused on the public sector. Should there be—because there's a number of amendments that have been suggested that we may bring forward later in a motion to the House. Would you recommend similar protections for children's privacy in the private sector or a higher level of protection for children's privacy in the private sector?

Mr. Prateek Sureka: At this point, what we really need is a foundational understanding of AI and building some trusted mechanisms in AI. We really commend that this bill is leading in the private sector—that would pave a great conduit for the private sector to come. But what we really need to see is a greater understanding of AI being implemented in the public sector in partnership with industry. And industry already has a number of gold standards being adopted in providing privacy protection for children and minorities.

Mr. Chris Glover: One of the other recommendations from the IPC is that there be no-go zones, and that this be ensconced in the legislation. For example, we shouldn't use AI systems to profile people for bail, we shouldn't use AI systems to profile people for social benefits, because we've seen what happened in Australia, where thousands of people were cut off of their social benefits. It shouldn't be used for scraping people's data.

Would you agree that there should be an outline of principle of no-go zones for AI in the legislation? Prateek?

Mr. Prateek Sureka: That's a tough one. One of the beneficial aspects of the provisions in the bill—the model has the provisions where the prospective regulations can focus on the creation of no zones for AI applications, setting a very clear boundary on what is not permissible by leaving room for innovation in other areas. But I think I'll repeat my point here: We need to start with setting gold standards for AI adoption in the public sector. And I think often good legislation has been defeated by bad regulations, so we should lead with good legislation—what we have right now.

As the technology adapts and evolves, we can look at regulations in creating no zones, but right now I don't think there should be any rough creating of no zones in the legislation as is.

Mr. Chris Glover: Okay. I'll pass it to my colleague.

The Chair (Mr. Lorne Coe): MPP Wong-Tam.

MPP Kristyn Wong-Tam: Just to clarify, the Information and Privacy Commissioner in her submission had specifically made a recommendation in schedule 2 that the government should be more specific in naming that children and youth's personal information should be classified as sensitive, because right now it does not say that.

So I just want to maybe get you folks on the record here. Do you believe that children's information should be specifically labelled and classified as sensitive in this bill?

Roxana?

Ms. Roxana Sultan: For me, the spirit of that notion certainly resonates. I think I'm not very well-qualified to speak to specific amendments in terms of the legislation, but I think the spirit is certainly reflected in what we're seeing in the legislation. As I said, I don't see any concern with bringing that out.

MPP Kristyn Wong-Tam: Thank you.

So, in legislation we need to be able to use words to describe what we mean. If we're not reading it in the spirit of what you undertake—to Technation representatives, if

it was your own child, do you believe their information should be deemed sensitive?

Mr. Prateek Sureka: Thank you, member, for the question. As a parent I'm very mindful of answering that question and I respect what the Information and Privacy Commissioner has submitted.

I think if we approach the bill with creating more caveats into the bill by creating a lot of regulations—adding more things that could be eventually regulated, or regulations could be created prospectively. But if you tried to do that right now, it would start stifling innovation. I think we should look at creating measures where one group of the population is already safeguarded in the current mechanisms in the bill.

So with that, I would say that I agree with Roxana that it's in the spirit of—we agree with what the Information and Privacy Commissioner has submitted, but I think the bill has enough mechanisms to protect data for children and vulnerable populations.

The Chair (Mr. Lorne Coe): Thank you for that response, sir.

We are now going to move to the government members, and I have MPP Bouma, please. When you're ready, sir.

Mr. Will Bouma: Chair, through you, I'd like to just have a chat with the Vector Institute. Roxana, I appreciate your submission, and I also appreciate the Vector Institute's willingness to work with our government on a host of issues over the last number of years.

I was intrigued by this, and I think we need to have a little bit of a conversation about this. This morning, we heard testimony that—or at least I got the impression; I didn't get a chance to ask questions about that—elected members, i.e. the minister, should not be in charge of oversight of the legislation and that should be taken into unelected bureaucracy, i.e. like in the privacy commissioner's office. What troubles me about that philosophical view is—

Mr. Chris Glover: Point of order, Mr. Speaker.

The Chair (Mr. Lorne Coe): No, no. We're not going to do that.

Carry on, please.

MPP Kristyn Wong-Tam: You haven't heard the point of order.

The Chair (Mr. Lorne Coe): Carry on with the question, please.

You're out of order.

Carry on with your question.

Mr. Will Bouma: If you'll permit me to get to it—because our parliamentary system of democracy is based on an executive branch and a legislative branch and a judicial branch, and I kind of reject the notion of a large administrative state that goes through that.

1330

In your testimony, you had suggested that you should work with the privacy commissioner on parts of this legislation and even reviewing AI. I was just wondering if you agree or disagree on whether that should be in the minister's office, the regulatory parts of this bill, or whether that should be outside of elected members' responsibility.

Ms. Roxana Sultan: That's an interesting question. Again, I'm not entirely qualified to speak to the how of the implementation. I think what we wanted to ensure is that as this legislation proceeds and we start to get more into the regulatory aspects of it, that is happening in consultation with the subject matter experts.

We see the opportunity here as, really, a partnership between government and industry experts like the Vector Institute to ensure that we land in the right place. This is very much a green space around the world. You know that governments are struggling to regulate and to legislate around complex technologies like AI that are evolving as quickly as they are. We see an opportunity here for a true partnered approach to how we actually implement the legislation, and the way in which it is framed right now allows us the flexibility to be able to do that.

So the recommendation coming forward from Vector is that we can really drive this in a way that is responsive to the technology continuing to evolve, and we expect that it will continue to evolve very quickly. The legislation gives us a framework for doing that, but the ability to actually drive that regulation at the forefront in a much more nimble and flexible way will be critical to ensure that we get this right.

Mr. Will Bouma: Just going back into that a little bit, then, on the ability for the legislation to be nimble, I remember when we were debating this legislation in the House, one of the criticisms that was raised constantly in the House was the fact that there was a lot of issues in this legislation that are left to regulation. The response to that is that we need to be able to be nimble in the minister's office to respond quickly to threats as they arise in this online space and with AI and technology changing so quickly.

My question is, then: In your opinion—and it's an opinion; that's fine. But from the Vector Institute's position, should we have to change legislation every single time a new threat comes up? Or is it much more appropriate for the people of Ontario for the ministry to be able to respond very quickly to threats as they arise, as quickly as possible in regulation, as opposed to having to wait for legislation to pass?

This legislation was introduced in the spring; it's November. Do you think a legislative process for every tweak to this legislation as risks arise is an appropriate way of dealing with this?

Ms. Roxana Sultan: That's exactly the perspective that we're taking, which is that it's prudent to keep legislation broadly defined enough and interoperable internationally, which is what we've advised on this particular legislation, so that we have that flexibility at the regulatory level. The more we can create structure around the legislation to allow that to happen, the more flexible, and more nimble and more responsive we'll be able to be as these winds continue to shift.

Mr. Will Bouma: Very good. Time?

The Chair (Mr. Lorne Coe): Two minutes and 29 seconds, sir.

Mr. Will Bouma: I will turn it over to my colleague, sir.

The Chair (Mr. Lorne Coe): MPP Riddell, please, when you're ready.

Mr. Brian Riddell: Technation has advocated for a regulatory approach that focuses on migrating reasonable, foreseeable harms from technology use. Can you elaborate on how you would believe the risk-based framework proposed in Bill 194 can be designed to effectively address these types of harms while providing the necessary flexibility?

The Chair (Mr. Lorne Coe): To the question, please.

Mr. Prateek Sureka: I can take that. Thank you, MPP Riddell, for that question. The Bill 194 risk-based framework is an effective approach because it addresses the potential harm in a way that is both proactive and adaptable. Rather than a rigid, one-size-fits-all regulation, the risk-based approach provides very tailored safeguards and different types of technologies, and their application ensures regulation remains relevant and appropriate.

The flexibility allows Ontarians and Ontario to set very clear guidelines for safety and security without stifling innovation in the tech sector, which is a very crucial balance for emerging technologies like AI.

Mr. Brian Riddell: Thank you for your answer. Time?

The Chair (Mr. Lorne Coe): You have one minute and eight seconds, sir.

Mr. Brian Riddell: What aspects of the bill do you believe would address concerns about the use of AI and, increasingly, the potential of cyber attacks?

Mr. Prateek Sureka: Thank you, member. We have heard about cyber security attacks in Canada writ large and in our province. As a very concerned citizen, a regular user of Toronto Public Library—which was hacked recently, and the website went down for a good six months. The services are still coming up fully functional.

Bill 194 very specifically addresses concerns about AI-fuelled cyber security threats by embedding AI within cyber security efforts. There is no government in the world that can create regulations and legislations faster than the technology that is evolving. But the Ontario government's efforts to ensure that AI advances too so that the tools defend, and increasingly sophisticated attacks—so, by embedding AI into the tools that would be deployed to defend our province and our country writ large, the bill's provisions emphasize the safe and responsible use of AI in cyber security—

The Chair (Mr. Lorne Coe): Thank you very much, sir. That concludes the time available in this round for government questions.

We're back to the official opposition, please. MPP Wong-Tam, when you're ready, please.

MPP Kristyn Wong-Tam: Thank you, everyone, for your presentations so far. I'm just interested in picking up a thread of question that MPP Bouma was going towards, and that was about who should provide oversight. There was, I think, a statement that perhaps government would be the best to provide oversight as opposed to an accountability officer. I think the guests who are appearing before us today—you are aware that this House, the Ontario Legislative Assembly, has different oversight offices, independent overseers of how we spend the province's finances, how members may conduct themselves adjacent to and abutting the code of conduct, oversight bodies with respect to how public services are delivered to the public and how they're received.

Do you support having an independent Information and Privacy Commissioner having oversight to this piece of legislation?

Roxana, I see you're thinking.

Ms. Roxana Sultan: Yes, I'm thinking. I think, again, from my perspective—I mean, I'm here as an AI industry expert, not as a legislative oversight expert. I don't feel I have sufficient information or knowledge to really be able to speak to that.

MPP Kristyn Wong-Tam: Okay. I can accept that. Thank you.

And for yourself? I want to bring in Mr. Lesani. You're on the screen, so I don't want you to feel neglected here. Perhaps you can offer us some comment to that question.

Mr. Fariborz Lesani: I'll follow the last comment: Again, my expertise isn't qualified to give feedback on this question.

MPP Kristyn Wong-Tam: Okay. Thank you, sir.

And then for you, perhaps, Ms. Mondou?

Ms. Angela Mondou: I'm going to defer to my policy expert on the left here, who is Prat.

Mr. Prateek Sureka: Thank you, member. I think I would chime with the other members, testifying that I'm not an expert on legislative oversight, but the legislative authority for ministers to issue directives to public sector entities is quite common in parliamentary democracies. I think I'll just kind of leave it at that.

MPP Kristyn Wong-Tam: Okay, fair—thank you very much. I appreciate that you are all coming in from the AI tech side of the sector. I know also, in speaking with those who move in the innovation circles, that they don't generally like too much regulation. Let businesses be business actors so innovation can happen in the margins.

Because we're at this committee and our purpose here is to ensure that this legislation comes out as strong as possible, to provide public institutions overall guidance on how to manage the different types of threats that exist today—not just cyber threats and not just AI as it rapidly develops faster than probably all our collective minds put together—but also to jump ahead into best practices of what we're seeing around the globe, ensuring that this legislation is not outdated as quickly as it's passed but forecasting what is to come. If we look at models around the world, we recognize that if we don't regulate—and regulation is just one piece of it, because then you have to go into the enforcement component, then you've got to put in time and energy and money, and then you've got to go through the judicial process to get your outcome. Because we are already behind the eight ball—the government has not acted fast enough to even get in front of digital literacy, as Mr. Lesani was saying in his deputation—we're really

far behind when it comes to developing statutes, regulation-monitoring and governing AI technology as it evolves.

1340

My question: Is it not prudent for us now to hopefully see regulations, or at least the intent of what these regulations are supposed to do, earlier as opposed to waiting for something that may or may not happen behind closed doors at the discretionary timeline of the minister? How do we catch up?

Ms. Roxana Sultan: I think, again, the way that the legislation is framed, and being able to have that ability to engage in a flexible way on the regulation, is a critical enabler for us. As I mentioned before, I think the opportunity really exists in being able to have a very coordinated approach to thinking through the regulation. Speaking on behalf of the Vector Institute, we are here as that resource. We are here to support that process and to support the government in driving that forward.

I think the opportunity to move quickly is certainly recognized, and certainly we are here to support in any way we can to enable that.

MPP Kristyn Wong-Tam: Thank you. I believe my colleague here would like the rest of the two minutes, Chair.

The Chair (Mr. Lorne Coe): MPP Glover, please.

Mr. Chris Glover: The government believes that the minister should make regulations that might or might not protect our children's privacy behind closed doors, and they object to even putting the principle that children's data should be classified as sensitive in legislation.

Mr. Lesani, do you believe that children's data should be classified as sensitive in this legislation?

Sorry, did you hear the question?

Mr. Fariborz Lesani: I heard the question; I was muted.

For sure, children's data—it depends on what we're referring to as data: images on the Internet or just public or private data in the public institutions or private institutions? They should be more secure. But the question is, does the adult information not need to be as secure as children's? If you have security in place for children, why not apply the same to everyone?

Mr. Chris Glover: Thank you so much.

Let's see, I've got one other question; I'm not going to be able to get too far into it. But procurement: I hear from many tech businesses in my area that they'd like to see a change because government procurement contracts open up all kinds of doors for them. When they're seeking out contracts internationally, if they have a government contract, it gives them legitimacy and they can get more.

What should the government be changing in terms of its procurement of tech resources?

Ms. Angela Mondou: I'm going to take this one on because I used to run a predictive analytics company and couldn't do business in Ontario or Canada.

First and foremost, modernization: Right now, the extent of the contractual implications can't keep up with the agility of the technology. Agile procurement is a process that is being adopted with governments around the world, and that's having procurement terms and conditions that are more rapidly—"flexible" is perhaps a better word—

The Chair (Mr. Lorne Coe): Thank you for that response. That concludes the official opposition's questions.

We'll now turn to the government, please. MPP Saunderson, when you're ready.

Mr. Brian Saunderson: Thank you to all the presenters today for your feedback and your expertise-sharing in the preparation of this legislation.

Ms. Mondou, I think in your comments you talked about Ontario being a leading jurisdiction in North America in the tech sector. Would you say that this legislation is actually cutting-edge in terms of the other jurisdictions in Canada?

Ms. Angela Mondou: I would say you're ahead of getting this legislation out, which makes it cutting-edge, yes.

Mr. Brian Saunderson: I appreciate that. You talked in your comments about the light-touch regulatory approach. We've heard how quickly—I'm sure, probably, in the three hours we've been at this committee, there have already been changes in the AI sector. So making changes—and we've heard that the legislative framework is a clunky thing, and you know that—so the regulatory responsiveness.

But I wanted to get a sense from each of you what a light regulatory approach would look like. I'll start with you, Ms. Mondou.

Ms. Angela Mondou: From my perspective, which is leading, not delivering or legislation, how I look at it is, there are sectors out there that have far more need to have more attention from a regulatory perspective than others. Logistics information for a trucking company may or may not be that sensitive; health care data is. Allowing a light-touch regulatory approach allows the flexibility to deliver regulation based on the sensitivity of the data.

Mr. Brian Saunderson: Thank you. Roxana?

Ms. Roxana Sultan: I think in terms of the approach to regulation, we need to look at what are our priority areas for regulation. If we think about the areas where there is greater sensitivity—direct impact of AI systems on citizens, particularly sensitive areas such as health care and children's services—of course, we would want to make sure that we're looking at it through that lens of transparency, accountability, fairness and bias. Are we implementing systems that are understandable and explainable, and we understand how they are making their decisions? Who holds the accountability for the decision-making of these automated systems? And then, obviously, when it comes to bias, are we ensuring that the outputs of these AI systems are not differential depending on who they're making decisions for and that they're not reinforcing the marginalization of any groups?

Those areas are where we can drive that regulatory lens around transparency, accountability and fairness, particularly in the more sensitive areas so we can prioritize accordingly.

Mr. Brian Saunderson: Thank you. Mr. Lesani?

Mr. Fariborz Lesani: Trying to understand these different forms of data is important, so that we decide what can be more flexible and what cannot be flexible. Items that can be more flexible, we can have less restrictions on them and address them as they come up, whereas for things that cannot be flexible, then we create legislation on those as fast as we can. That would keep changing, but at least if we have the high-priority items addressed right away, it would probably help.

Mr. Brian Saunderson: Thank you.

The Chair (Mr. Lorne Coe): MPP Riddell, please.

Mr. Brian Saunderson: If I could?

The Chair (Mr. Lorne Coe): Okay. Go ahead.

Mr. Brian Saunderson: Mr. Chair, just before I move on, this will be my last question. Prateek, you spoke in your comments about setting the gold standard in the public sector before we venture into the private sector. I'm wondering if you could just take us through the rationale for that, and how that evolution might come into play.

Mr. Prateek Sureka: Thank you, member. That's a great question. We understand the need for flexibility, enabling a framework of technology as technology evolves really rapidly. We support the approach taken in Bill 194.

A prescriptive regulatory approach could really hinder innovation and, as this technology is really nascent and still finding its foot and still being deployed, I think putting that in the public sector will welcome a structure that allows room for growth while establishing essential safeguards and protecting minorities, children and the groups there.

Collaboration with the public sector would be absolutely essential and would be key in shaping these further regulations to balance safety and flexibility. As the public sector leads the deployment of artificial intelligence in partnership with the private sector, there's a lot of room for ongoing partnership and industry, which has been really strong so far. We must continue to ensure that the regulations stay relevant and effective.

By light-touch regulation, the regulations give a lot of flexibility to adapt to the technologies as they're evolving. As you rightly said, by the time we've had this hearing, AI has already moved by leaps and bounds.

Mr. Brian Saunderson: It's too bad we can't do the same thing.

Thank you very much for your answers, everyone. Those are my questions.

The Chair (Mr. Lorne Coe): All right, thank you.

MPP Riddell, please. You've got 2:08.

Mr. Brian Riddell: Technation has emphasized the important roles technology and industry can play in building public trust in AI. From your perspective, how can the private sector collaborate with government under the framework proposed in Bill 194 to facilitate the responsible adoption and use of AI, particularly within the public sector?

Mr. Prateek Sureka: I can take that, if that's okay, Angela?

Ms. Angela Mondou: Sure.

Mr. Prateek Sureka: Yes, all right, and I'll pass it on to you. We'll take turns.

The private sector can collaborate really effectively with government by leading in areas such as public education, safe experimentation and change management, and I think Angela is going to allude to change management in just a bit.

Just to elaborate a little bit on public education, by providing expertise and resources, the tech industry can really help the public sector build foundational knowledge about AI, demystifying its functions and applications for civil servants and the public alike.

Angela, do you want to allude to the change management part?

Ms. Angela Mondou: I'll start by saying that in my experience, the public sector has described itself, to me, as being very risk-averse. I do think that when it comes to the public sector and AI adoption, you really need to look at the approach of, how do you engage the public sector to become less risk-averse?

Back to what Prat was referring to, there is a change management requirement there. That's something that the tech sector does across Canada and around the world: embrace and work with large organizations of tens of thousands of people to move them forward.

I think that in terms of some of the important steps that need to be taken, we've talked about education. There's creating tiger teams within an operation, people that in the public sector embrace AI and can help move forward across the organization. There's obviously the training and the connection around that for the employees and also the understanding of how their job will or will not be impacted—

The Chair (Mr. Lorne Coe): Thank you very much for that response. That concludes the government's time for the questions.

Thank you all for being with us this afternoon. The committee will be in recess until 2 o'clock.

The committee recessed from 1352 to 1400.

PROOFPOINT
COUNCIL OF CANADIAN INNOVATORS
MR. LOGAN SHIELDS

The Chair (Mr. Lorne Coe): The Standing Committee on Justice Policy will continue with its sitting. Our next presenters, members, are Proofpoint, the Council of Canadian Innovators and Logan Shields, who is joining us by Zoom, I believe. Is that correct?

Those presenters that are with us now, you have seven minutes to present. If you don't get finished in seven minutes, I'll interrupt you and go to the next presenter.

Please state your name for Hansard, and you may begin your presentation, please. Thank you.

Interjection.

The Chair (Mr. Lorne Coe): Yes, please. Thank you. You need to identify yourself, and then I know. All right? Go ahead.

Mr. Robert Mackett: I will. Sorry, Mr. Chair.

The Chair (Mr. Lorne Coe): All right. Thank you.

Mr. Robert Mackett: Good afternoon, Mr. Chair and committee members. My name is Robert Mackett. I'm vice-president and country leader for Proofpoint Canada. Thank you for the opportunity to present today as you discuss and hear from those of us in the cyber security industry regarding Bill 194.

Proofpoint is a leading cyber security and compliance company used by more than 85% of the Fortune 100 and prominent research universities, global retailers, pharmaceutical companies and financial institutions, to name a few. We specialize in human-centric security, protecting organizations' people from advanced cyber threats while defending the data that they create. With over 500,000 customers worldwide, Proofpoint's human-centric cyber security platform provides organizations with a modern security architecture to stop targeted threats against their people, safeguard information and digital communications, provide employees with continuous guidance towards safe behaviours, and contain application and identity sprawl. Our company is on the front line of today's evolving cyber security threats, detecting and stopping trillions of threat activities every day.

We're here today to express our support for Bill 194 and highlight why we believe this legislation is necessary to improve the cyber security posture of Ontario's broader public sector and strengthen Ontarians' data privacy. We share a similar goal to the Ontario government: improve the cyber security posture of Ontario's broader service institutions and safeguard the data of Ontarians. We're proud to serve Ontario's broader public sector through a wide suite of services and solutions.

Any organization can be a victim of a cyber attack. Ontario's broader public sector, much like the rest of the world, is becoming more digital, remote and data-driven. Across Ontario and globally, today's cyber attacks are targeting people. Three in four data breaches rely on exploiting the human element, and 95% of cyber security issues can be traced to human action. In fact, in our 2024 Voice of the CISO report, more than four in five Canadian CISOs identified human error as their organization's leading cyber security risk, and 90% of Canadian CISOs feel at risk of experiencing a material cyber attack in the next 12 months, compared to 58% in 2023. Canadian CISOs indicate the leading cyber security threats facing their organization are business email compromise, cloud account compromise and supply chain attacks.

Between 2018 and 2022, Ontario businesses reported 180% more cyber security incidents, with the average data breach costing Canadian organizations approximately $6.3 million. Without proper safeguards, cyber threats in our province and globally pose a real and present danger to the safety and security of critical infrastructure, sensitive personal data, intellectual property and financial systems.

The introduction of Bill 194 is a significant step by the Ontario government to strengthen cyber security programs in the public sector. It builds upon the government's cyber security strategy, which was introduced in 2019. From our experience, every organization and company has a different cyber security posture and capabilities, determined by the resources and funding available to that entity. While many larger organizations are taking proactive steps with risk and maturity assessments, smaller organizations face challenges, due to limited access to shared resources and expertise. It's clear that the government realizes the risk that this reality presents. It is why we're glad to see that the legislation before us today empowers the Ministry of Public and Business Service Delivery to lead the cyber security direction for select public sector entities, especially for those vulnerable sectors like children's aid societies.

The legislation also creates a centralized reporting mechanism to respond to cyber security incidents, a measure that we firmly believe will elevate the overall maturity of Ontario's cyber security regime. It will not only increase the maturity across the broader public sector, but will also enable the government to respond rapidly to threats and take a macro lens to cyber security across the province to identify threat actors and respond accordingly.

In closing, Mr. Chair, we believe this legislation is necessary to improve the cyber security posture of Ontario's broader public sector and strengthen Ontarians' data privacy. We commend the government of Ontario for taking this critical step and look forward to continuing our work and lending our global expertise to ensure that the government continues to lead on reducing risks to cyber threats.

The Chair (Mr. Lorne Coe): Our next presenter is from the Council of Canadian Innovators. We need your name, then you can start.

Ms. Skaidra Puodžiūnas: Good afternoon, Chair and members of the Standing Committee on Justice Policy. Thank you for the opportunity to present on Bill 194. My name is Skaidra Puodžiūnas, and I am the director of Ontario affairs for the Council of Canadian Innovators, a national business association representing more than 150 of Canada's fastest-growing technology companies.

More than half of CCI's members are proudly headquartered right here in Ontario, employing more than 30,000 workers and contributing nearly $7 billion to Ontario's economy. Our CEOs are job and wealth creators, investors, community philanthropists, and experts in their fields of artificial intelligence, health technology, clean technology, financial technology, cyber security and more.

CCI commends the government's commitment to enabling guardrails for trust in the digital age, with an initial focus on public sector, and we urgently call on the Ontario government to involve the domestic innovator community as this important work evolves. With Bill 194, this is a historic opportunity to lay out a path for safety and clear regulation with the flexibility, innovation and economic potential that Ontario needs to seize right now.

And so, for the purpose of today, I want to hit on three key points: firstly, the importance of standards; secondly, ensuring that the market's platforms and products remain open; and thirdly, engaging and adopting Ontario innovation.

Embracing standards, firstly, can free up government capacity to focus on important priorities and allow innovators a degree of regulatory capacity and certainty. Standards can also present opportunities to create foundational building-block technologies that many other companies rely on. Even with the accelerating pace of change and different families of technologies, from semiconductor design to AI, standards bodies are working hard to create and keep up to date countless standards that ensure quality and keep people safe.

We encourage additional language in Bill 194 authorizing ministers to recognize standards as statutory instruments, if they are satisfied that they have been developed fairly and transparently through a process led by a standards development organization accredited by the Standards Council of Canada, Digital Governance Council or similar standards development organizations. This flexibility already exists in Ontario's recent laws, having been included in the Modernizing Ontario for People and Businesses Act in 2020, and would allow for regulatory innovation while also protecting citizen and user rights.

Secondly, keeping markets, platforms and products open: Smaller companies are particularly dependent on access to data. Rigid data minimization laws benefit large, established companies and prevent new market entrants from reaching customers and gathering the information they need to compete and succeed. Ontario's governance frameworks should incentivize data portability and data access: for example, open on-board diagnostic ports in automobiles that enable vehicle owners to upload data on their vehicles to any supplier who can help them process that data.

And thirdly, engaging and adopting made-in-Ontario innovation: Procurement is the most powerful economic development tool available to the government. Ontario spends nearly $30 billion annually in procuring goods and services, from pencils to complex medical technologies. When a firm in Ontario sells goods or services to the provincial government, it is considered a major validator for the company—one that helps acquire investors, accelerates future sales with other governments and businesses across Canada and globally. Bill 194 has the opportunity to open vast new networks to deploy cyber security and AI technologies across the broader public sector. So we call on Ontario public officials to consider the Ontario market first.

1410

Ontario's innovation problems are not due to the lack of commercialized and market-ready innovations but the adoption of them. The lack of a dedicated system to evaluate and fund innovation across the public sector has a direct impact on the local economy. Let's take a look at why this matters. Ontario's economy is seeing a profound shift, foundationally different from the traditional production-based commodities of physical goods which dominated the 20th century. Today, over 90% of the value of S&P 500 companies comes from intangible assets, things like data, patents, algorithms and copyrighted works. For a number of reasons, the intangible economy operates very differently from a traditional production economy. Strictly speaking, tech companies don't actually sell products; they amass data and intellectual property and then extract economic rents by allowing customers to use these systems.

Let's actually look at a recent example in Ontario. Just this month, the Ontario government issued a request for proposals to supply software to provincial call and contact centres, including ServiceOntario and the Family Responsibility Office, mandating the use of Amazon Web Services. Let's assume the government's due diligence leading up to the RFP confirmed that this was the most viable provider, with no Canadian alternative capable of delivering widespread cloud services for Ontarians. Even so, in this scenario, the government isn't just buying a product for the next five years. Mandating the use of AWS means that other companies who interface with these services must write software and format data to a standard established by Amazon. This gives a large-platform company enormous control and ability to shape the marketplace to their benefit.

This is a pivotal moment for Ontario to demonstrate accountability by actively consulting and collaborating with domestic innovators, because investing in Ontario's innovation ecosystem is not just economically sound, it's a strategic imperative for our province's future. Building up domestic companies does more than create new products; it attracts significant capital, generates high-value jobs, builds the foundation for future economic growth, and in the delivery of our public services—

The Chair (Mr. Lorne Coe): You have one minute remaining.

Ms. Skaidra Puodžiūnas: Thank you.

These companies are invested in protecting and driving value for citizens, because their employees are citizens.

As always, we appreciate your interest in our organization's advocacy. We do commend the government in moving forward with Bill 194 and look forward to further dialogue about how we can increase Ontario's innovation outputs while building a stronger and more inclusive economy for all.

Thank you for your time. I look forward to any questions you may have.

The Chair (Mr. Lorne Coe): Thank you very much for your presentation.

Our next presenter is Logan Shields. Mr. Shields is going to call in by telephone, right, Clerk? All right.

Mr. Shields, if you're on the line, you've got seven minutes to make your presentation. That will be followed with questions. Mr. Shields, please.

Mr. Logan Shields: Hello.

The Chair (Mr. Lorne Coe): Hello, Mr. Shields. It's Lorne Coe, the Chair of the committee. Can you start your presentation, please? You've got seven minutes. Thank you, sir.

Mr. Logan Shields: Hello. I want to share my perspective as a minor as to how this bill will [*inaudible*] digital technology [*inaudible*] for minors in Ontario.

First, I want to thank the committee for the opportunity to present. I want to make clear from the beginning that I

oppose targeting digital security protection based on age. I think all Ontarians deserve privacy protections and digital security, and targeting measures based on age ensures that not all Ontarians will have the same protections.

The bill seems to want to advance the privacy of Ontarians, but it doesn't affect some of the problems with the Freedom of Information and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act to provide safeguards for children's information, because under those acts children do not have the same rights as others to be involved in the collection, use and disclosure of their personal information. Because what does cyber security mean when you're not involved in the process for choosing who can have access to your information in the first place? Even after I turned 16—it can still be difficult to have a say in the collection, use, and disclosure of your own personal information, in my experience, when it comes to public sector institutions like my school.

The powers that the bill would grant concerning minors are very broad and could be used to restrict minors rather than to protect their information. The bill could be interpreted to give the government the power to require schools, school boards, and children's aid societies to regulate and restrict the use of digital technology by the children who receive services from them and to actually limit children under 16 from being involved in the collection, use, and disclosure of their personal information more than they already are.

Given how the current rules and laws are, I don't necessarily think that these new powers will be used in the interests of minors. The government has already used other powers to restrict children's technology use. Under the Education Act, the minister made a policy program memorandum to ban some children from using their phones during the school day at all, even at lunch, without the approval of their teachers. But no exception is made in this policy for contacting the office of the Ombudsman or the Information and Privacy Commissioner. Bad things happen if students feel unsafe at their schools and they don't think their school is helping them. Under other policies which the government has used to regulate digital technology, they can't use their digital technology to contact anyone. This policy program memorandum was published, but directives under this proposed act do not have to be published.

I strongly advise the committee to consider amending this bill to protect children and prevent the powers that this bill would grant from being used in a similar way to the other powers. For example, one of these regulations could be that schools should only contact the person with custody about the collection, use, retention and disclosure of personal information about children, and not the child. A directive could restrict children from using school or CAS computers to contact anyone, including the office of the Ombudsman or the Information and Privacy Commissioner.

This bill's preamble states that the government of Ontario "recognizes the importance of protecting the privacy of the people of Ontario and the value of enhancing Ontario's privacy safeguards through increased transparency and independent oversight." Sections 9 to 11 of schedule 1 are contrary to this purpose, furthering the double standard where children are sidelined. Giving power to restrict children's rights in an environment where independent oversight is already restricted through other policies that already exist—through directives that do not have to be published—goes directly against this purpose.

Although this bill has some problems, there are some steps that this bill takes in the right direction, but these steps don't apply to school boards—most of them; for example, the requirement to conduct privacy impact assessments and to report breaches of security safeguards, or the complaints process for security safeguard breaches. None of those would apply to municipal institutions like school boards or municipalities, which means that even when this bill does get stuff right, it's still not really going to affect students that much, or children.

Overall, I hope the direction the committee takes is ensuring a consistent increase in protection across all public institutions, including MFIPPA institutions and children's aid societies in Ontario, and removing the discriminatory provisions which will inhibit the bill from achieving its goals. I encourage the committee to amend the bill to achieve these purposes so that this can be a good bill to protect the privacy of the people of Ontario.

The Chair (Mr. Lorne Coe): Thank you, Mr. Shields. We appreciate that.

We're now going to move to questions from the official opposition.

1420

Mr. Chris Glover: Thank you, everybody, for coming and deputing today.

I'll start with Mr. Shields. Mr. Shields, are you a student? You said you're a minor, I believe.

Mr. Logan Shields: Hello. I am not currently a student. I was a student last year, but now I'm being homeschooled.

Mr. Chris Glover: Okay. Well, look, I appreciate—it's a very impressive presentation that you've given. I hope you will submit it in writing so that we can take a more detailed look at some of the recommendations that you're making.

The gist of what I got from what you're saying is that you oppose the targeting of digital protection based on age because it could be used to actually restrict children's or minors' access to their own data. Is that generally the theme that you're building on?

Mr. Logan Shields: Yes.

Mr. Chris Glover: Yes? Okay. Well, thank you so much for that. Be sure to submit it in writing so that we can take a look at this because we're going to be going over this over the next few days to develop amendments. Thank you.

I want to ask Ms. Puodžiūnas—could you say it?

Ms. Skaidra Puodžiūnas: Puodžiūnas.

Mr. Chris Glover: Puodžiūnas?

Ms. Skaidra Puodžiūnas: Yes.

Mr. Chris Glover: Okay, Puodžiūnas. My apologies.

Let's see. You mentioned procurement and you talked about the mandate—the government using an Amazon service for a recent procurement project. What would it have looked like if they had chosen a small or medium-sized Ontario tech company? What would it have meant to that company?

Ms. Skaidra Puodžiūnas: Thanks for the question. Look, I think cloud-providing services are a bit of a nuanced discussion. There are really only a handful of cloud service providers for the North American market, and so I can't comment on that specific. But what I will say is, we're just really looking forward to understanding more about how this decision was arrived at by the government and also, moving forward, the ways that the domestic community can gain business out of this decision. I think it goes without saying that even just the mention of a business name in an RFP goes a long way for validating that business, for giving more business and visibility to that business. So really just thinking about the opportunities ahead for the domestic community, I know there's many. It's just a matter of continuing to consider us for these types of procurements and RFQs that lead up to them moving forward.

Mr. Chris Glover: Okay. Certainly, it's a theme that I hear often from tech companies in the area that I represent and tech companies that I talk to, about the importance of government procurement, because it does give them legitimacy, especially if they're seeking overseas contracts, because then they can say, "Hey, we've got a government"—in fact, it's often one of the first questions they get asked when they're seeking an outside contract.

Let's see. You were talking about needing guardrails for trust. One of the recommendations from the Information and Privacy Commissioner this morning was that the legislation be amended to include a declaration of principles that would state that these principles should assert that AI should be used in a manner that is valid and reliable, safe, privacy-protecting, transparent, accountable and human rights-affirming. Would you agree with that principle being embedded into the legislation?

Ms. Skaidra Puodžiūnas: Absolutely. Time and time again, we hear from innovators that they really want to go about it from a responsible AI approach. Also, the regulatory certainty actually enables innovation because they know where the direction of government is going and how they can collaborate and work with government going forward. So, 100%, we'd want to see those principles in action and we'd want to be supportive wherever we can.

Mr. Chris Glover: Okay. Thank you so much.

I want to go to—sorry, I'm just skimming through my notes here—Mr. Mackett. You were talking about providing a suite of services. Let's talk about cyber security. You were talking about small public agencies, particularly—and this is what I've heard; I've spoken with a number of small public agencies, and they say they do not have the wherewithal or the financial means to actually provide the kind of cyber security that they want for the data that they're protecting.

What should be done in order to protect our public data that's held by small public sector agencies?

Mr. Robert Mackett: Great question. I think it starts—and this is where Bill 194 begins the dialogue on what that strategy needs to be, where we need to prioritize our efforts, where the areas of biggest risk are. In looking at where those data sources are—and there are organizations that are struggling with it, in how to enable the best vehicles, the best strategy and prioritize work efforts in and around that.

I think it's no one-size-fits-all in this space, certainly, and I don't think that this bill actually pretends to that, which is why it's so good to have the focus at this time to start that dialogue and determine how to—

Mr. Chris Glover: In your work with cyber security, especially small public sector agencies—one of the things that I've been told is that cyber security criminals will target public sector agencies that they know are poorly funded. Certainly, our hospitals are struggling right now. Our universities are struggling.

Does the lack of funding for these agencies make them a target for cyber security attacks?

Mr. Robert Mackett: It absolutely can have impact. I think we look at ministries like Ontario health, where they have gone through the similar path, and what we've seen very much in the health sector—they've done an admirable job, over the course of the last 12 to 18 months, building out a framework, setting priorities and establishing models by which they can create centres of excellence to deliver exactly that: services to broader ecosystems.

Hospitals are not in the business of cyber security. They're in the business of saving lives, delivering vaccines. So aggregating and creating strategies to support the smaller aspects—

Mr. Brian Riddell: Point of order.

The Chair (Mr. Lorne Coe): Yes?

Mr. Brian Riddell: We're not talking about funding. We're talking about this bill.

The Chair (Mr. Lorne Coe): Agreed.

Back to the scope.

Mr. Chris Glover: Amount of time?

The Chair (Mr. Lorne Coe): You have 54 seconds.

Mr. Chris Glover: Thank you.

I want to go back to this procurement piece. What could that procurement with Amazon have meant for a small Ontario-based company?

Mr. Robert Mackett: It's a challenging question to ask—and I think my colleague up here spoke eloquently on that. There are a core set of providers that have become almost de facto standards in delivering quality of service in that space. However, what can be interesting is the layering-on of Canadian companies and organizations, on top of those types of services, into what we need to do in the government space.

The Chair (Mr. Lorne Coe): The government: MPP Riddell, please.

Mr. Brian Riddell: My question is for Proofpoint. What is your organization doing internally to address cyber security concerns and to raise awareness?

Mr. Robert Mackett: Great question.

We provide several free resources, reports and tools to support organizations, to raise cyber security awareness. We're just coming off of Cyber Security Awareness Month in October. So we continue the conversations long after that's over—candid conversations with both private sector and government agencies around how we can better and constantly evolve to address the modern threats that impact the BPS—

Mr. Brian Riddell: But what do you do internally to do that? How do you achieve that?

Mr. Robert Mackett: Very, very specifically, we have programs in and around security awareness training. So we start looking at how organizations—we talked very much, in my address, around people being the weakest link; focusing on human-centric security. Part of it is not just the tools that are in place; it's about the technology and the people who are leveraging it.

Garnering awareness for organizations, whether it's in the private sector, whether it's in the public sector, is one of the first places that we start engaging with organizations to help defend against some of the modern threats that are facing businesses and our most impactful institutions today.

Mr. Brian Riddell: So what is your opinion on the bill? Do you support it?

Mr. Robert Mackett: Absolutely. I think, first and foremost, Bill 194 starts a dialogue. It starts the focus on cyber security so that we can up-level and upskill Ontario to be ready for modern threats, to protect our critical infrastructure, to correct those institutions that we serve—the broader public and the private sector, as well.

Mr. Brian Riddell: My thoughts on it are, it's changing every day, and we need to have the ability to address it every day. This is written into the bill too, so the minister will have that ability to do so. You would agree with that too?

Mr. Robert Mackett: Absolutely. It's flexible. It allows us to be dynamic in the way that we respond. Even in sessions such as this with committee, we can engage in discussions with both public and private sector entities and partners like Proofpoint to determine the path forward, not only to learn what to put in place that works, but also, conversely, to understand what's failed in other jurisdictions so we don't make the same mistake.

1430

Mr. Brian Riddell: Live and learn.

Mr. Robert Mackett: Live and learn, exactly.

Mr. Brian Riddell: Thank you very much.

Mr. Robert Mackett: You're welcome.

Mr. Brian Riddell: I'll hand it over to Effie.

The Chair (Mr. Lorne Coe): MPP Triantafilopoulos.

Ms. Effie J. Triantafilopoulos: My first question is for you, Robert. And thank you both and the other individual who's online for us.

For my first question, I wondered if you could elaborate on how mandatory cyber incident reporting under Bill 194 could enhance Ontario's cyber security landscape and the role that Proofpoint could play in supporting compliance and risk mitigation.

Mr. Robert Mackett: That's a great question. Thank you very much.

Mr. Chair and committee members, I think it's important to recognize that it's a real stigma to report failure. It's a stigma, potentially, for smaller organizations to report a cyber incident in the same way. By having an independent body having visibility to that, it will provide awareness for the government, by and large, to reduce the impact to Ontarians' data across the province. By not having it, we don't know what the impacts could be and it provides a greater sense of risk to our businesses as a whole in Ontario.

Ms. Effie J. Triantafilopoulos: Thank you.

This question is for you, Skaidra. I'm really excited by your enthusiasm and your describing what our domestic innovators do and the strategic imperative around supporting them, making sure that our—and I loved the way you described that the intangibles today are actually our goods and services of yesterday.

Just from your perspective, what key considerations would inform a tailored, scalable cyber security framework that could be used for various levels of government as well under Bill 194? And with the innovation ecosystem in mind, how might Bill 194 further harmonize security and privacy standards without stifling the competitiveness that you've been talking about?

Ms. Skaidra Puodžiūnas: That's a great question. I think that's the core of this exercise, right? I think it all comes down to the approach—you know, the way in which this bill unfolds. I would agree with my fellow colleague—I don't know; what do I call you?

Interjection: Witness.

Ms. Skaidra Puodžiūnas: Witness, thank you.

This legislation does start a conversation, and the devil will be in the details, so we do see this as enabling legislation. But the regulations that will follow will exactly answer these questions of: How do we actually marry the standards that have been presented on the privacy front to actually create a cyber framework that will work for the domestic community?

I think it, again, goes back to involving us in consultations, involving domestic voices from every step of the way. The pillars and the needs are not all that transformably different. There still needs to be access to the best talent. There still needs to be access to the greatest customers—so thinking about procurement. And there still needs to be access to capital. We just have to think of it a little bit differently. We have to think of it from a modular perspective. We have to think of it from a changing and dynamic perspective, and we have to think about the geopolitics at play. The results of the US election are going to impact our approach to cyber infrastructure and cyber security and privacy regulation.

Thinking about cloud, thinking about where data lives, and the access that certain governments have and the relationships and bids that government forms with these other countries—these are things that we have to think about at the offset as we develop. I think it's sort of an invitation for us to be a part of the dialogue, to be a part of that framework development, and for us to also give you tangible research—

The Chair (Mr. Lorne Coe): You have one minute left.

Ms. Skaidra Puodžiūnas: Sorry. So, yes, I would just say it's all in the approach and all in the lens which we put forward as we get granular on it.

Ms. Effie J. Triantafilopoulos: Both of you are at the forefront of that, and many of us are just trying to educate ourselves and trying to keep up.

How would we go about helping to demystify AI to the broader audience? What are some of the suggestions you have going forward? I'll ask both of you.

Mr. Robert Mackett: I'm going to defer to my colleague, who's an expert on AI. I speak more to cyber.

Ms. Skaidra Puodžiūnas: Oh, I'm an expert on AI?

Interjection.

Ms. Skaidra Puodžiūnas: I think it just goes back to the stories we tell, right? So I have a handful of companies that use AI and have been working with the public sector for a number of years, whether it's from a talent development workforce perspective or it's helping educators in school boards. There are so many great examples of AI making public sector jobs easier, creating efficiencies, creating productivity, but we have to enable it and we have to really look for the stories—

The Chair (Mr. Lorne Coe): Thank you very much for that response.

We're back to the official opposition.

Ms. Skaidra Puodžiūnas: Thank you.

The Chair (Mr. Lorne Coe): MPP Wong-Tam, please, thank you. When you're ready.

MPP Kristyn Wong-Tam: This has been an extremely illuminating conversation. I'm interested in drilling down a little bit deeper about the storage of information.

So our data—the government has some information sitting on servers. As we move into the cloud platform, it's no longer sitting on physical servers owned by the government. Considering that the clouds are oftentimes not even in the country, if they are not in Ontario or out of Canada, the local jurisdiction or local nation-state will have their own set of regulations and statutes that govern how that data is managed.

So, ultimately, who owns the data? And when there are conflicting laws on the point of procurement, the point of entry to where it's stored, which body of legislation will prevail? My question is to all our esteemed speakers.

Mr. Robert Mackett: It's a great question. I, unfortunately, am not an expert in legislation, so I'm going to have to defer answering that question.

Ms. Skaidra Puodžiūnas: I think these are the right questions. I think these are questions that a lot of our companies are wrestling with as well, who have business and provide services to multiple governments.

I think it's important to know where the data lives. I think it's important to also know how the data is being accessed, and what is not only the legislation that governments are putting forward, but the accountability metrics in place. You can say that this is the legislation, but what is the actual governance model? What are the actual consequences or repercussions for not following that model? Time and time again, we see large, foreign-national players that grow and grow and grow in certain digital and data spaces and kind of look the other way when it comes to legislation.

I think it's creating a culture of trust. I think it's bringing many players in to the table, but I think it's also having a bit of guts and courage to not take on a certain procurement because it goes against Canadian values or Canadian direction. So just really thinking about these questions at the offset is really, really important.

MPP Kristyn Wong-Tam: Thank you.

Mr. Robert Mackett: If I can just make one more comment on that: I think the world has changed radically over the course of the last 12 to 18 months—even 24. I think a lot of the core providers that the government could be evaluating in that space do have presence in Canada, do have the ability to put some of the guardrails in place that we might be looking for to be more effective custodians of Ontarians' data in some way, shape or form.

So I think if we peel the onion back a little bit further, outside of the legislation itself, if you're specifically talking about procurement activities and how to make sure we're keeping Ontarians' data safe, there are vehicles and options that are in place today that can move beyond the legislation if we're just looking at how we want to control and manage the data that we have access to.

MPP Kristyn Wong-Tam: Thank you.

Earlier, MPP Riddell said on a point of order that this bill has very little to do with funding, and I think that is absolutely correct, but the bill does download some burdens on public institutions on how they need to manage the data and collect the data and who has access. For public institutions, it may not be within their sweet spot of service delivery. It's not necessarily within their expertise; they oftentimes will have to contract out and issue RFPs for vendors that are qualified, and then we see that they're asking for AWS-friendly suppliers.

When that happens, ultimately there will be some burden of cost, because it's specifically an impact of the bill. What do we do when public institutions are asked to do more work that they are not, in all honesty, probably qualified to do, or they don't have the means to hire the qualified people to execute and yet they're asked to do that? What do you think will happen?

Mr. Brian Riddell: Point of order.

The Chair (Mr. Lorne Coe): I have a point of order.

Mr. Brian Riddell: It's out of scope, this question.

The Chair (Mr. Lorne Coe): I didn't hear you.

Mr. Brian Riddell: This question from MPP Wong-Tam is out of scope.

The Chair (Mr. Lorne Coe): Just bring it back, please.

MPP Kristyn Wong-Tam: Absolutely, Chair. I'm trying to understand the impact of this legislation asking public agencies to undertake certain performances as outlined in the bill. How would they do that work if they're not resourced to do so?

1440

Mr. Robert Mackett: Well, if I may, my understanding of the bill itself is it's starting that dialogue between the various parties. It doesn't actually dictate a one-size-fits-all approach to smaller agencies that might not be equipped to handle that, but it starts building out a strategy and having the right discussions to move up the maturity scale as it relates to protecting these agencies, boards, commissions and entities in the broader public sector—moving them up the maturity scale.

MPP Kristyn Wong-Tam: Is it your understanding that it's an opt-in process for these public agencies? Can they just ignore the legislation if they don't have the resources to undertake this work?

Mr. Robert Mackett: I wouldn't say that that is my understanding at this time, but if we don't start the discussion now, we're going to be pushing that down the hill, down the road. I don't think we have the luxury of time to do that right now.

MPP Kristyn Wong-Tam: So it is foreseeable that the good intentions of the legislation that will provide guardrails may not be actually implementable, if the public institutions don't have the means to actually execute.

I'm curious to know—with respect to keeping Ontarians' data safe, there was some talk about the sensitive nature, especially for minors. They don't have, necessarily, agency over all of their information. We recognize that teachers are talking about them, doctors are talking about them. They are sending information back and forth to each other—health providers.

The IPC recommended a classification that was going to highlight the vulnerability of minors. It didn't seem like a controversial matter, but I'm hearing from you that perhaps it's not the best approach. Did I understand you correctly? Or do you believe that minors should be treated differently and that their data should be protected as sensitive data?

The Chair (Mr. Lorne Coe): You have 37 seconds for an answer.

Mr. Logan Shields: Well, I do think it is more sensitive. But I think that's as a result of the laws that allow—it's more based on the current laws around how it's handled rather than an inherent fact about the information. Because under the current laws, children don't even know when their information is being collected, so how would they know how to protect it when they don't know it's even out there?

The Chair (Mr. Lorne Coe): Thank you very much.

We're back to the government for questions, please. MPP Saunderson, when you're ready.

Mr. Brian Saunderson: I want to thank all the presenters on this panel, or witnesses, as you put it, for your comments today—it's very helpful—and for sharing your expertise with us.

I'd like to start off with Skaidra. Hopefully, I said that right. I take to heart your comments that we have a huge growing tech sector in Ontario. I think we're probably one of the fastest-growing tech sectors in North America over the last 18 months. We heard from prior witnesses that this legislation is—we're a leading jurisdiction and this legislation would put us at the forefront. Do you agree with that?

Ms. Skaidra Puodžiūnas: Yes, we would. In many ways, Ontario is starting a conversation that a lot of provinces across Canada have not put in such a way, so I think it would be right to say that Ontario is leading a really important discussion with this legislation, and we're really excited to be a part of that.

Mr. Brian Saunderson: It's interesting that you use the word "discussion," because prior witnesses also talked about how quickly this landscape changes and that by doing some of this through the regulatory approach, it's more iterative. And it's a light regulatory approach that will allow us to be responsive and target certain areas that are going to require attention, versus others that may not require that same level of attention. You would agree with that?

Ms. Skaidra Puodžiūnas: Yes.

Mr. Brian Saunderson: You had three issues that you wanted us to consider. One was the development of standards across the industry and then market accessibility, to keep Ontario companies in there, and then also embracing Ontario technology.

I'm wondering if you can talk a bit, because we have mentioned procurement, but not on, sort of, the global sense—but just the opportunity. Do you think this legislation would provide opportunity for Ontario tech companies to get involved in how we address, and how we maintain, cyber security and AI?

Ms. Skaidra Puodžiūnas: Yes, 100%. I think this, again, is transformative, because it is accessing an entirely new market in many ways. It's also a call on rethinking the delivery of public services and rethinking how we support public institutions in this transition.

As was mentioned by opposition, we are thinking about how to support the public sector, and I think this is an opportunity to think about the private sector's role in educating, in training and also just ensuring that there is a co-creation of a path forward. As this is operationalized, I think this is an opportunity to bring in ministries of health and Ontario Health and other sectors that would be impacted by this legislation. So I think the role for Ontario is absolutely massive.

Mr. Brian Saunderson: Thank you very much for that.

Robert, asking you sort of the same question from a cyber security perspective: Does this open up opportunities for Ontario businesses?

Mr. Robert Mackett: It's absolutely a huge opportunity. When we talk about uplevelling and upscaling in Ontario, the opportunities are quite limitless. And much like you've identified, the threat landscape is constantly

evolving, so we collectively have to remain vigilant. We must ensure that we've got the right skills out there, the right capabilities, in order to do so. So I think, yes, it's absolutely a great opportunity.

Mr. Brian Saunderson: Is it fair to say, then, that not only is this legislation going to push the needle forward in terms of protecting data for Ontarians and getting our foot in the door on AI and how we monitor that moving forward, but it's also going to open up opportunities for providers in Ontario?

Mr. Robert Mackett: Significantly, absolutely.

Mr. Brian Saunderson: Great. Thank you very much. Those are my questions.

The Chair (Mr. Lorne Coe): I have MPP Riddell, please, sir.

Mr. Brian Riddell: Can you speak about the importance of mandatory cyber incident reporting and what your thoughts are?

I'll ask you first on that.

Mr. Robert Mackett: It's a great question. Thank you for asking that. I think I made mention of it previously, but if we don't have mandatory reporting, we run the risk of having more risk in the ecosystem, broader impacts, tougher time remediating the issues that are out there, and we lose the ability to learn from some of the challenges that other organizations might face. It's a great opportunity for us as the government to be able to start getting ahead of some of the challenges, to move quicker on some of the things that we need to do in and around this space. So I think it's absolutely critical.

I talked about having a stigma that's associated with it. By forcing, or at least implementing that approach, it will remove that stigma because it will be part of what we need to do each and every day.

Mr. Brian Riddell: It will become commonplace.

Mr. Robert Mackett: It will become commonplace.

Ms. Skaidra Puodžiūnas: It's absolutely important that there's an acknowledgement of when a cyber attack happens, that there's a mechanism for reporting it, of course. I think that legislation gets at the heart of that. I think—less fussed on the specific tactic, but moreover, again, this legislation just puts a really deep focus on cyber education, cyber responsiveness. This is something that our public sector institutions absolutely need to be a part of and need to be roped into.

So I'm really supportive of those principles that are outlined in the legislation.

The Chair (Mr. Lorne Coe): You have a minute and 52 seconds. Other questions, please?

Mr. Brian Riddell: How might these proposals and requirements, as part of Bill 194, encourage the development and growth of Ontario's cyber security industry?

I'll start over here. It's a big question.

Mr. Robert Mackett: It's a big question. You're making me think here.

The legislation provides a focus on cyber security that we really desperately need in Ontario. It's critical to uplevel our skill industry and get ahead of the threats that are facing our vital broader public sector partners and institutions.

Ms. Skaidra Puodžiūnas: As somebody who has also spent a lot of time outside of Canada, in countries like Estonia and in Finland and other parts of the world that are deemed global cyber security experts, it's absolutely critical that Ontario has something in legislation and it's absolutely critical that we work hand in hand with public institutions, as well as private sector institutions.

By moving forward with this, it opens up a lot of discussions around operationalization of this, about how to actually effectively upskill our public sector workforce about what the role of government is in the digital age. I think this is the direction that we're heading, and so for Ontario to be a part of it is really the essence of this legislation; it's that we're moving forward and that we're thinking about how to buy in the digital age, how to train in the digital age, how to report in the digital age, and thinking about how to invest in the digital age and in our economy.

1450

So yes to that question. It opens up an entire array of opportunity, and I think Ontario has this opportunity to also look at other jurisdictions—

The Chair (Mr. Lorne Coe): Thank you very much for your answer. Thank you to the government side.

Thank you for all your presentations today, and have a great afternoon.

ONTARIO HUMAN RIGHTS COMMISSION
KYNDRYL CANADA
DELL TECHNOLOGIES CANADA

The Chair (Mr. Lorne Coe): We're now going to move on to our 3 o'clock presenters, because they're here. You can all come up to the table when you're able to, please. Thanks again for being here. Dell Technologies Canada, the Ontario Human Rights Commission, and Kyndryl Canada, please come on up.

You're going to have seven minutes each for your presentation. When you're about to start your presentation, please state your name for Hansard—that's the official recording service of the Legislative Assembly of Ontario—and you may begin. Who would like to go first? Hands up?

Ms. Patricia DeGuire: I shall start first.

The Chair (Mr. Lorne Coe): All right. Thank you. Your name, please?

Ms. Patricia DeGuire: Patricia DeGuire, chief commissioner of the Ontario Human Rights Commission.

The Chair (Mr. Lorne Coe): Thank you. You have seven minutes for your presentation, and I'll let you know when that seven minutes has finished. Okay? Thank you. You can start, please.

Ms. Patricia DeGuire: Good afternoon, legislators, and thank you for inviting the commission to provide an oral submission on Bill 194. I shall limit my submissions to the proposed provisions of the public sector's use of

artificial intelligence. Human rights in Ontario, as expressed in the Ontario Human Rights Code, are fundamental, quasi-constitutional, and require that all Ontario legislation, regulations, policies, procedures, and programs, including this bill, be consistent with the code.

The commission has been monitoring the development of digital technologies and their impact on human rights for many years. Integrating a human rights-based approach works for the public interest, including regulators, businesses, government, ministries, and its ongoing work with the Ministry of Public and Business Service Delivery and Procurement to advocate for strong AI guidance.

Bill 194 is a positive start, given its stated goals. There are key elements, however, that the bill needs to address to ensure that the opportunities, benefits and attendant protections of AI are available to all Ontarians without discrimination. I shall make four key points, and I refer you to the commission's submissions that were submitted earlier.

Human rights protections are necessary to prevent predictable and unforeseen harms from AI. The use of AI by public sector entities around the world has already resulted in serious harm to individuals and communities, including discrimination based on race, gender, and other personal attributes. The use of AI technologies has produced and, in some cases, intensified discrimination. For example, across the United States in its health system, using AI for risk scoring, fewer resources were allocated to Black patients compared to white patients with the same level of need.

In the Netherlands, as well, 20,000 families were wrongly investigated by the country's tax authority using an algorithmic system for fraudulently claiming child benefit allowances. It was reported that tens of thousands of families, often with lower income or belonging to ethnic minorities, were pushed into poverty because of the exorbitant debts to the tax agency. Some victims even committed suicide, and more than 1,000 children were taken into care. As outlined in the commission's written submission, there are many more examples which have led to tragic and harmful results.

Legislation rooted in human rights will protect Ontarian communities while advancing economic opportunities. When AI benefits and its attendant use protections are available to all Ontarians without discrimination, I guarantee you Ontario benefits economically. Recognizing human rights protection is vital to Ontario's economic prosperity. The Organisation for Economic Co-operation and Development has made human rights one of its five AI principles: "Promote use of AI that is innovative and trustworthy and that respects human rights and democratic values."

Some jurisdictions are passing AI legislation, which prioritizes human rights to proactively align with international standards, thus positioning themselves to attract investment and be seen as leaders in AI ethical spaces. Ontario can be a leader by creating a robust regulatory ecosystem that helps local talent develop AI products and services that appeal to customers across the globe.

The commission's recommendations are vital to addressing foundational concerns in Bill 194. Bill 194 doesn't reference human rights and the protection under the Human Rights Code. Legislators, these protections must be embedded in the legislation itself, like you did in the Comprehensive Ontario Police Services Act. Let me quote: "The importance of safeguarding the fundamental rights and freedoms guaranteed by the Canadian Charter of Rights and Freedoms and the Human Rights Code." That's one of its principles.

Also, the commission recommends that the government embed a principles-based approach to AI regulations, asserting that AI should be vital, reliable, safe, privacy-protective, transparent, accountable and human rights-affirming. Bill 194 should include regulations that set out expandability requirements for AI systems before they can be used. The EU and the US have done this already. They are committed. Bill 194 must establish clear no-go zones for AI technologies and be clear about the government's role and how it will respond in the public interest if public sector entities continue to use technology that proves unreliable, unsafe and unlawful.

The Acting Chair (Mr. Will Bouma): One minute.

Ms. Patricia DeGuire: Finally, Bill 194 must include policing and social assistance services as focus areas, given their impact on marginalized communities and previously designated areas of schools, children's aid societies and hospitals.

Lastly, implementation recommendations resulting in consultation: We say that it's essential to consult—it is more important to implement. It is important that the results of consultation, including with the commission and other regulatory bodies, experts and communities, should be implemented in the future draft of the legislation.

In sum, the foundational nature of the commission's recommendations requires these inclusions in the legislation itself rather than in the regulations. Legislators, Ontario is a leader in human rights. It can maintain that leadership by embedding human rights principles in the use of AI. Thank you so much, and we're happy to answer questions, if you have questions.

The Acting Chair (Mr. Will Bouma): Perfect timing.

We will now move on to the presentation from Kyndryl Canada. Go ahead. You have the floor—seven minutes.

Mr. Denis Villeneuve: No worries, thank you. My name is Denis Villeneuve. I'm the security and resilience practice leader for Kyndryl Canada. I'm also the co-chair of the Indigenous working group within Kyndryl as well, and a member of the Peter Ballantyne Cree Nation.

On behalf of Kyndryl Canada, committee members, we appreciate the opportunity to appear before the Standing Committee on Justice Policy to provide our feedback on the Ontario government's Bill 194. We appreciate the government's efforts to bring greater security, transparency and public trust to its public services. Kyndryl understands the importance of cyber regulations and believes they can be beneficial for all. They establish a standardized framework for cyber security and data protection, both of which foster trust and confidence in digital trans-

actions and services. By requiring organizations to adopt robust security and resiliency measures, and to manage cyber risks effectively, regulations help mitigate the potential for significant losses and disruptions.

For context, Kyndryl operates in over 60 countries with 78,000 employees globally. We have 4,000 customers worldwide, including 60% of the Fortune 100 and more than half of the Fortune 500. Kyndryl Canada is headquartered in—well, we've just moved south of Steeles, so in Toronto, Ontario. We have about 2,000 employees across the country. We have several data centres across the country. And, most notably, we have our security operations centre in Barrie, Ontario.

1500

One of the biggest privileges we have, as a global company, is our proximity to our customers and their mission-critical operations. We build, operate and manage the technology that thousands of businesses and governments around the world depend on every single day to run smoothly and securely, enabling our customers to better serve their customers. We also serve regional and national governments as they modernize operations and extend new services to their citizens, and we help protect personal data, national security, and strengthen their economies.

Because of our global position and our relationship with mission-critical enterprises, we get to see the whole threat landscape in global trends as it relates to cyber. In our inaugural global study with exclusive data from our AI-powered Kyndryl Bridge, which gives us end-to-end visibility of a client's entire IT estate, it shows how Canadian executives rank risks, prioritize investments, and balance technology and talent. Our Kyndryl Readiness Report stated that 89% of Canadian leaders are confident in IT, but only 34% say it's future-ready. Security, macroeconomic uncertainty and regulations top lists of Canadian executives' concerns. AI return on investment, limited skills compliance and compatibility, end-of-life technology are some of the top challenges of Canadian CEOs. Compared to its global counterparts, Canada ranks among the lowest in IT readiness, with more than two thirds, 68%, concerned about their organization's ability to adapt to emerging threats. Yet, while 93% of Canadian leaders say technology modernization is a high priority for their companies, data from Kyndryl shows that almost half of all mission-critical IT infrastructure globally—44%—is approaching end of life, and the increasing vulnerability and raising barriers to modernization is very important. Government infrastructure is included in that stat.

With that in mind, we provide the following recommendations, under schedule 1, with cyber security:

First, begin with the end in mind. What is the minimum viable operation of that organization? It could be a minimum viable bank, minimum viable province, minimum viable committee—whatever it may be. With cyber threats on the rise, resilience is more important than ever, so, having that cyber resilience plan in mind, we do suggest using a recovery plan similar to the United States' NIST SP 800-184—if you want some bedtime reading. It's very important to follow what others have done in other markets.

Secondly, implement a zero-trust framework to enhance protections—zero trust is to trust no one implicitly, always verify. This involves a shift in mindset in a lot of organizations, and it requires the governance structures to be able to implement it correctly. The CIS framework in the United States, as well as the DOD, Department of Defense, do have very good recommendations in that regard.

Thirdly, a risk-based vulnerability management program is a cyber security practice that proactively aims to identify and remediate vulnerabilities that pose risks to an organization—and risk-based must consider the vulnerabilities that are actively being exploited in the wild to gain a foothold within organizations today, and then understanding what those vulnerabilities can link to in regard to critical infrastructure, critical data.

Fourth would be implementing third-party risk management. Third parties are the weakest link in many organizations, and understanding how to actively mitigate your risks with third parties that have access to your organizations is very important.

Last but not least, modernize legacy infrastructure, and implement compensating controls if you cannot modernize. There are lots of people out there who have that issue.

The Chair (Mr. Lorne Coe): You have one minute, sir.

Mr. Denis Villeneuve: Well, to that end, we at Kyndryl understand the importance of the government's proposed legislation to protect Ontarians through the strengthening of cyber security and building trust in the public sector.

In response to the bill, we are well positioned to support the objectives of the bill, and with expertise in cyber security, responsible AI and data privacy, as the bill progresses, we look forward to providing our continued collaboration to help build a stronger and better Ontario.

The Chair (Mr. Lorne Coe): Thank you, sir, for that.

Our next speaker, please. Your name, and you can start. Thank you.

Ms. Pamela Pelletier: Wonderful. Thank you. Pamela Pelletier, and I am the vice-president and country lead for Dell Technologies here in Canada. Thank you for the opportunity to comment on Bill 194.

Dell Technologies—Dell—has been a leading business here in Canada for over 35 years. Our headquarters are here in Ontario. Over 1,100 of the 1,500 employees working for Dell in Canada are in Ontario, making the province home to the majority of our employees in Canada. Over the decades, we've continued to invest significantly in Canada, in Ontario specifically, including the creation of a logistics hub in Brampton and, more recently, a 5G research facility in Ottawa.

We're proud of the long-standing relationship with our customers in Ontario, serving over 2,000 major accounts across the public and private sectors, with many thousands more small businesses as well as consumers here in Canada.

We have a long-standing partnership with the Ontario government as a trusted vendor, and we look forward to continued engagement in these important policy issues. We'd like to thank the government for taking a leadership role on the issue of public sector oversight related to artificial intelligence and cyber security.

With technological advancements continuing to progress at breakneck speed, it's critical for policy to keep in lockstep with these developments and take into consideration and account the diverse new concerns. Bill 194 takes an important step in that direction, requiring public sector entities to provide information to the public, develop and implement an accountability framework and take steps to manage risk with the use of AI systems.

Dell supports this legislative effort to improve the regulatory AI and cyber security landscape. If implemented, this legislation will be an important step towards increasing security and predictability for citizens and other stakeholders in the AI and cyber space.

Dell provides the infrastructure for AI. We create technology solutions that help organizations modernize their IT across clouds, data centres and at the edge. We help manage and protect their data, modernize work and keep people and organizations connected. AI allows digital systems to perform tasks commonly accomplished by humans. This includes things like solving complex problems, automating tasks, enhancing efficiency and productivity, and it also helps improve decision-making.

AI is one of the most powerful innovations in productivity that we've seen in the modern technology era. Upwards of a 20% to 30% lift in productivity is anticipated. That potential is driving a race to innovate and invest in AI models across all industries.

Dell helps customers accelerate that adoption of AI with the right support and technology along their entire AI journey, from strategizing, implementing, adopting to scaling AI projects. One of our key enablers is our enormous open ecosystem of strategic partners that help simplify the complexity of AI developments. In addition to providing the infrastructure to run AI, we're a connector that leverages our ecosystem of innovative partners and customers to accelerate their deployments.

While global AI regulations are primarily focused on risk mitigation, it's vital that they provide the space needed for innovation and drive the development of existing emerging industries for sustainable human and economic progress. Regulations should not impede AI innovation and the efficient fulfillment of its enormous potential.

AI is moving at an incredible pace. For government to keep up with this growth, policy guardrails should be flexible and include regular evaluation. As governments evaluate the future of AI, maintaining an adaptable and predictable regulatory path will ensure smooth progress. It's critical that flexibility in regulation and regular evaluation is built in from the onset to put AI policy on a pathway that can adapt and evolve through technological needs and international collaboration.

1510

Bill 194 takes an important step by defining AI broadly, to capture a variety of machine-based systems that generate a variety of outputs with the ability to influence different environments, allowing for such flexibility. And the catch-all in the definition to include other systems not specifically enumerated will allow the legislation to remain relevant through continuing technological advancements.

AI does not operate in isolation from other major technology domains such as data, cloud computing, privacy and security. We recommend that AI policy always consider its dependencies and impact on policies in these other domains. Cyber security, ethics and privacy are some of those areas that need to be considered.

In 2023 we announced our new ESG trust pillar, which is a three-pronged strategy inclusive of privacy, security and ethics and compliance. In listening to our customers, we realized how important these key aspects are in building trust. Privacy, security and ethics are especially important in building trust when it comes to the use and creation of new technologies like AI. We make it a priority to design, develop and deliver secure IT products and solutions. Security and privacy are built into all that we do from our supply chain assurance capabilities to all phases of our secure development—

The Chair (Mr. Lorne Coe): You have one minute left.

Ms. Pamela Pelletier: One minute? I'm going to skip to the end then.

Dell applauds the government for raising the importance of cyber security in the face of increasing digital attacks. By investing public and private sector time, attention and resources, together we can build a resilient future. With regulatory harmonization and effective collaboration, public and private, we can enhance the digital ecosystem. The provisions in Bill 194, empowering the development and implementation of these programs, ensure cyber security as well as regulating the technical standards.

Finally, the taxpayers also greatly benefit from the government's effective use of AI in cyber security tools. Passing this legislation will create an enabling regulatory environment that will allow Ontario residents to benefit. Thank you for your time.

The Chair (Mr. Lorne Coe): Thank you very much.

We are now going to move to questions from the members of the official opposition, please. MPP Glover, sir, when you're ready.

Mr. Chris Glover: Thank you all for your presentation today and thank you for taking the time to be out here. It's a really important part of our democratic process to have these committee hearings, and to hear from the public about what amendments could be made to this bill to make it stronger and to better protect our data privacy, and also to seek some of the opportunities from AI.

I'll ask my first question of Ms. DeGuire. You mentioned that AI should be available to all Ontarians without discrimination. Are you talking about the digital divide?

Ms. Patricia DeGuire: What I'm going to do at this juncture—and just to correct, the name is DeGuire.

Mr. Chris Glover: DeGuire. I apologize.

Ms. Patricia DeGuire: I'm going to yield to—I brought two tech gurus with me today, and I think they'd be up to respond to that question. It seems rather technical to me.

Mr. Alfred Fung: My name is Alfred Fung. I'm a senior policy analyst at the Ontario Human Rights Commission. Just to respond to your question with an example—it's about the digital divide. It's about making sure that the opportunities presented by AI are available to everyone in Ontario without discrimination.

An example of that I would give is, in the United Kingdom they have the National Health Service. They use an algorithmic system to determine who gets liver transplants in the country. They sort people based on need, and whoever is at the top score gets the next liver. The problem with the system was that basically anyone below the age of 45 could not get a liver because the algorithmic system determined that if you are below the age of 45, you'll live longer than a person that's over the age of 45. But the administrators of the system weren't aware of that; it actually required someone who is on the list to examine the issue, fortunately, because data was available about the function of the system.

I bring that up because it wasn't a situation that was about any particular group of people. It was discriminating against the people—the whole country—based on age. It was age discrimination, right? Those are the types of concerns that we're talking about. It's not just to ensure that marginalized and vulnerable communities are protected; we're talking about all of us as well.

Mr. Chris Glover: Thank you for that.

Let me just ask a subsequent question, then. The Information and Privacy Commissioner has recommended an amendment to the bill: that we add in these principles that should assert that AI should be used in a manner that is valid and reliable, safe, provides privacy protection, is transparent, accountable and human rights-affirming. Is it that kind of discrimination that leads us to have to need or require this "human rights-affirming" statement be put into the bill?

Mr. Alfred Fung: Yes, so where we're talking about keeping flexible in the legislation and the regulation, we are recommending that the legislation have these principles so that public sector entities are aware that these are the foundational principles that they need to be aware of when they're procuring these technologies, operating them, reviewing them.

Again, back to the age example: If you don't list human rights as a foundational principle in the bill, they probably would not have considered age as a concern when they were testing and reviewing these systems. That's why we're talking about the principles that we referred to, the same ones that the IPC referred to earlier. That's why we're saying they're so important.

Mr. Chris Glover: Thank you. Time check?

The Chair (Mr. Lorne Coe): You have 3:11 left.

Mr. Chris Glover: Okay.

The EU Artificial Intelligence Act classifies AI systems into four risk categories to address the varying degrees of potential harm and ethical risk: unacceptable risk, high risk, limited risk and minimal risk.

Should this bill also incorporate a risk assessment for AI technology?

Mr. Alfred Fung: I'll pass that over to my colleague Jagtaran Singh. While he comes up, I'll note that, yes, the EU recommends impact assessments for high-risk systems, which is actually to the point why the OHRC released the impact assessment recently.

Mr. Chris Glover: Okay. Thank you.

The Chair (Mr. Lorne Coe): Mr. Singh, please attend the table. And for the record, your name, please, and your position.

Mr. Jagtaran Singh: My name is Jagtaran Singh, and I am counsel at the Ontario Human Rights Commission.

The Chair (Mr. Lorne Coe): Thank you, sir. To the question.

Mr. Jagtaran Singh: Right. So the EU, as you mentioned, certainly has various risk-based systems. We've seen that appear in alternative legislation that's being proposed federally as well. It's one route to go and it's certainly a way that we can help categorize.

I think our concern, at this point, is less with the risk-based system and more with the fact that human rights aren't even mentioned in the bill itself. Just to bring that back to our main submission, which is essentially that we can have risk-based systems, we can have various accountability mechanisms, but these need to be mentioned in the legislation itself and not simply relegated to the regulations. Appreciating the need to be nimble, there are certain foundational issues that need to be addressed in the legislation and that touch on human rights concerns. Risk, accountability, transparency: These are some of them.

Mr. Chris Glover: Okay. Let me ask another question. The Information and Privacy Commissioner recommended that we need an amendment in this bill to protect children's data, and that children's data should be deemed sensitive and given a higher level of protection.

Does the Human Rights Commission agree with that?

Ms. Patricia DeGuire: Thank you for your question. Children are the most vulnerable, I would say, in our communities. Oftentimes, even legislation has to be implemented to protect them from their very parents, regrettably. I think that the state has that inherent responsibility to protect them through whatever laws that are there to protect them. Human rights and privacy protection legislation are key legislation.

Just to be clear, the Human Rights Commission is not saying that all of this is bad. What the Human Rights Commission is essentially saying to you honourable legislators is this: Human rights are fundamental to all of us, and we need to embed that in the legislation to protect the most vulnerable—

The Chair (Mr. Lorne Coe): Thank you very much. That's the questions from the first round, at least, for the official opposition.

1520

I'm back to the government members, and I have MPP Saunderson. Sir, when you're ready.

Mr. Brian Saunderson: Thank you to all our presenters for sharing your expertise and time with us today.

Commissioner DeGuire, I'm going to start with you. I know you're busy. Hopefully you won't have to play musical chairs, but if you need to, please go right ahead.

I wanted to get a bit of background from you on the work that you, the OHRC, and the law commission did on a human rights AI impact assessment tool. Can you tell us a bit about how that came to be and what you found?

Ms. Patricia DeGuire: I'm going to say one thing: I approved it. I'm going to defer to the gentlemen who were working on it.

Mr. Brian Saunderson: Okay.

Ms. Patricia DeGuire: Approved because I understood—but let the workers speak. Thank you.

Mr. Alfred Fung: Just on the impact assessment: We developed it in collaboration with the Law Commission of Ontario, who will be presenting tomorrow, so they can probably provide even more detail. But basically, we saw from engagement with public and private sector entities that there was a clear need for organizations to understand their obligations under the Ontario Human Rights Code, but also under the Canadian Human Rights Act—just what are human rights, right? The tool is designed to be a step-by-step to help them navigate through the questions of where their systems might, for example, interact with personal characteristics that are protected under the Human Rights Code: for example, age, as I mentioned earlier.

Basically, what we learned through this process is that there is a clear need to emphasize the importance of human rights in these processes where there might be a focus on bias, there might be a focus on making sure that it doesn't discriminate against certain groups. But ultimately, there needs to be guidance or an emphasis on the principles of human rights that are important to all of us, which is why the code has primacy above all other legislation.

Mr. Brian Saunderson: It's interesting that you should raise that. I appreciate what you're saying, but you just finished off by saying that the Ontario Human Rights Code has primacy over all provincial legislation. So would you agree with me that whether or not we put in the statement about the dignity, the Human Rights Code actually prevails and overarches all of this legislation, so Bill 194 is subject to the Ontario Human Rights Code in any event?

Mr. Alfred Fung: I'll pass that over to our legal colleagues that can answer that question.

Ms. Patricia DeGuire: I think that's an interesting concept, but, really, that's not the way it works. The Human Rights Code itself, which is a piece of legislation passed by government, takes those decisions that whenever—legislation, regulation—you must consider it. It's a positive obligation. So just to leave it and say that it will be there is not good enough. It's not good enough because we all vowed to be the protectors of all inherent rights, and we who are in the power positions to do that must demonstrate that in every which way we can.

Legislators, you have the honour of doing that in legislation, and I would urge you to do it. Don't leave your constituents to assume that it's there, because the courts will tell you that unless something is written in the legislation, it wasn't meant to be. They go back as far as Hansard to see what was discussed in Hansard to see if that was in contemplation. Now you have the honour to do it. I urge you to do it.

Mr. Brian Saunderson: I appreciate your answer, and I certainly recognize your constitutional law authority on that, so thank you.

I just want to dig down a little more on this, because we're hearing how quickly this landscape changes, and probably in the time we've been here discussing AI today, there's been changes that are happening way faster than we can pass legislation and regulations.

Your associate talked about how nimble we need to be, but if we incorporate your AI assessment tool into the regulations and embed it in there, will that help to address—because I'm learning a lot. I'm learning today what an LLM is. I used to think that was a law degree, but I understand now it's language, and it changes so quickly, and that it can embed bias by the information it gets.

What you've been talking about and your associates have been talking about is how AI can generate a bias that will be discriminatory in its ultimate decision-making processes at the end, and that's something we want to avoid and stop and snuff out. I appreciate what you're telling us.

By using your assessment tool in how we draft our regulations, that would be helpful, wouldn't it?

Ms. Patricia DeGuire: It would be helpful. But I'll also say something that came all the way back from 1947, from Lord Sankey: Legislation changes, and the people who administer it should be nimble and be able to pivot when these things happen.

While you have a guideline that might be good today—we are the people who created it. We also must be nimble. We must be apprised and keep changing it. And we are prepared to do that, because life is not static. That is why it is so important to embed these principles, because while things may change rapidly, principles generally hold on for a longer time. But it is the intention to keep on reviewing and making changes to that, and changes should never be a reason for people not to do the right thing.

Mr. Brian Saunderson: It seems like this is an area where change is happening at unprecedented speed.

Ms. Patricia DeGuire: All the time—real time, too.

The Chair (Mr. Lorne Coe): MPP Riddell. You've got 42 seconds, sir.

Mr. Brian Riddell: I had some questions for you, Denis. I think I'll wait till the next round. I just found it really interesting when you started talking about legacy infrastructures, and one of my questions was going to be: How do you handle a company that has old software?

The Chair (Mr. Lorne Coe): You've got 11 seconds, sir. You might want to save that for the next round.

Mr. Brian Riddell: We'll save it for the next one.

The Chair (Mr. Lorne Coe): I'm going to go to the official opposition, please. MPP Glover.

Mr. Chris Glover: Thank you, all, for being here.

I just want to address one other question to the human rights commissioner. You mentioned the importance of human rights and that the Human Rights Code is automatically embedded in every piece of legislation. However, Bill 28, introduced by this government in 2022, specifically used the "notwithstanding" clause to override the Canadian Charter of Rights and Freedoms, including our fundamental freedoms and our legal rights of education workers—

Mr. Will Bouma: Point of order.

The Chair (Mr. Lorne Coe): MPP Bouma, go ahead, please.

Mr. Will Bouma: Could we get back to the bill at hand?

The Chair (Mr. Lorne Coe): I agree.

I cautioned, at the beginning, that I wanted to deal with the scope of the bill. You're outside of the bill. That's my ruling.

Carry on, please, with a new question.

Mr. Chris Glover: I want to ask, if the Human Rights Code is automatically embedded in every piece of legislation, including this piece of legislation, at a future date could the government introduce a piece of legislation that applies despite the Human Rights Code, as they did with Bill 28?

Mr. Will Bouma: Point of order, please.

The Chair (Mr. Lorne Coe): Point of order, please.

Mr. Will Bouma: We're speaking about the bill at hand, not about a hypothetical future bill.

The Chair (Mr. Lorne Coe): I concur again.

Restate your question. Bring it back to the scope of the bill, please. You're outside of the bill, sir.

Mr. Chris Glover: There's a proposal to incorporate into this bill that AI be used in a way that is concurrent or coincides with the Human Rights Code. This government has used legislation to override the Human Rights Code. The government just argued that the Human Rights Code is automatically embedded in any legislation. This can be overridden. So my question is—

Mr. Will Bouma: Point of order.

The Chair (Mr. Lorne Coe): Point of order, please.

Mr. Will Bouma: If the member opposite wants to—

Mr. Chris Glover: Obviously, you don't want an answer to this question, because you're—

Interjections.

The Chair (Mr. Lorne Coe): I just need to hear one person at a time.

Mr. Saunderson.

1530

Mr. Brian Saunderson: The Ontario rights code has primacy over all provincial legislation. All provincial legislation must comply with the Ontario Human Rights Code. Commissioner DeGuire is a constitutional lawyer—

Interjections.

The Chair (Mr. Lorne Coe): Hold on. Hold on. I'm not going to have cross-debate.

I've already ruled three times already that you're outside of the scope of the bill. You are again. One more time, and I'll rule you out of order, okay?

Let's go. State your question.

Mr. Chris Glover: I'll pass it to my colleagues. It's obvious they don't want an answer to this question even though they raised the subject.

The Chair (Mr. Lorne Coe): MPP Wong-Tam, please.

MPP Kristyn Wong-Tam: With respect to international law as it relates to human rights—just because I think there is a very important issue and it deserves our serious attention—the 1948 Universal Declaration of Human Rights and other legal instruments recognize the right to privacy as a fundamental human right. Canada, as a signatory—we have Canadian laws, the Canadian charter of freedoms, that also stipulate the same thing, and now we have the Ontario code.

And because this issue is of importance, and the minister earlier today—I know you didn't have the privilege of hearing his deputation, but when asked whether or not he would embed and put a human rights lens over this, as recommended by 45 different other organizations that support and defend civil liberties in this country, the minister was unable to answer the question. He just couldn't quite nail it down by saying, yes, he believes that this legislation needs to have a human rights approach.

Commissioner DeGuire, you are telling us specifically that if it is not embedded in the legislation, it's simply not there. Is that my understanding of what you said?

Ms. Patricia DeGuire: I am here urging the government as the chief commissioner of the Ontario Human Rights Commission that the code must be followed. All legislation, programs etc. must be in compliance with it, and were a legislation to say that the code doesn't apply, it still must comply with charter principles. So whether it's the code or the charter, there is a requirement, a positive obligation, to respond to the code or the charter or both.

I hope I answered your question.

MPP Kristyn Wong-Tam: Yes. It's crystal clear for me. I just wanted to have it on the record so everybody on our committee can understand what the obligations of the government are. Thank you.

Just coming back to the practical application of this act: We do recognize that things are rapidly changing. It's taken us a lot of time just to deliberate this one tiny, little legal matter, but we didn't necessarily—we need to ensure that the good intentions of this legislation don't necessarily stop only at public institutions. It starts there, but I think that we probably need to extend the rule of law as it pertains to privacy collection, AI, facial recognition and the whole—everything that falls under that umbrella; we need to be able to provide some guardrails, language that has been used today.

To our two guests who are coming from Dell Technologies, as well as Kyndryl Canada: The role that the private sector has to play in ensuring good legislation to protect the public—what do you see your role as? Starting with Dell Canada—and I'm very happy to say I'm using a Dell laptop today.

Ms. Pamela Pelletier: Thank you. I think the role is to work together. So engagement with the private sector from the public is critical and will have the best outcomes. Some areas like information sharing, partnerships—I think partnerships are key, and if you look at partnerships from a Canadian perspective, we sometimes lag, so partnerships would be a key area. Standardization is important, and then, of course, best practices. There are definitely synergies between the public and private, and so coming together on those would be important.

MPP Kristyn Wong-Tam: Thank you. I've got 33 seconds left, and I want to squeeze in one more question, so I want to make sure you get this very special question. We have seen in other countries where there is a push to have an independent regulator or independent governance accountability officer. We heard earlier that the Information and Privacy Commissioner will have some responsibility, but it's not going directly to her office—

The Chair (Mr. Lorne Coe): Thank you very much, MPP Wong-Tam. Your time for the official opposition has concluded. You might want to recharge your watch on that iPhone. The Clerk has a very accurate eye for—

MPP Kristyn Wong-Tam: No, I'm not disputing it, sir.

The Chair (Mr. Lorne Coe): There we go.

MPP Kristyn Wong-Tam: I'm just looking at my iPhone. I'm just looking at my technology.

The Chair (Mr. Lorne Coe): All right. We have the government now, and I have MPP Riddell.

Mr. Brian Riddell: Back to Denis Villeneuve: As a leader in cyber security and resiliency solutions, your company has developed a deep expertise in protecting critical digital infrastructure. Can you provide some insights on the type of high-risk AI cases that you believe the regulatory framework proposed in Bill 194 could address?

Mr. Denis Villeneuve: In regard to high-risk AI, from a Kyndryl perspective, we believe the EU act is definitely leading from a global perspective, and we are actively relying on that, for them to be leading the way. So what they're doing is what we agree with from that perspective. Does that help?

In regard to cyber security risks of AI, it's same, same but different. You've got OWASP Top Ten type of ways of breaking into web applications. You've got OWASP Top Ten vulnerabilities of breaking into LLMs and AI modules. It's taking the same type of lens to AI.

Mr. Brian Riddell: Now I'll go to the question I was going to ask you prior. It was about legacy infrastructure programs. How do you deal with that when you have a customer that is using outdated software?

Mr. Denis Villeneuve: First and foremost, it is a priority to modernize legacy infrastructure because once something is no longer supported by a vendor, there are no longer patches or anything that comes out in order to protect. So the more legacy infrastructure you get, it's just a snowball effect of more and more vulnerabilities being available to nefarious actors to take advantage of.

When prioritization or budgets don't allow to modernize an entire infrastructure, mitigating controls or compensating controls are very important. I've seen in industry where mitigating controls were only applied in areas where there were compliance requirements, but then, in other areas of their infrastructure, they didn't do microsegmentation, as an example, where basically, it just segments the vulnerabilities from one another so there can't be just taking full advantage of the entire infrastructure. So, (1), priority is on modernization because of the snowball effect and the broader vulnerability, and then, (2), it's the mitigating controls that need to be in place.

Mr. Brian Riddell: Thank you for your answer. Now I will ask all three of you. In your opinion, do you support this bill?

Mr. Denis Villeneuve: Yes.

Ms. Pamela Pelletier: Yes.

Ms. Patricia DeGuire: Yes, implementing human rights considerations.

Mr. Brian Riddell: Thank you. Because of the changes in AI happening on a minute-by-minute basis, we need to have someone that can be on the spot and react to that. So do you agree that the minister should have the ability to make those changes?

Mr. Denis Villeneuve: Yes.

Ms. Pamela Pelletier: Yes.

Ms. Patricia DeGuire: The minister should follow their conventions of passing legislation.

Mr. Brian Riddell: Thank you for your answers. I will now pass it to Stéphane.

Le Président (M. Lorne Coe): MPP Sarrazin, à vous.

M. Stéphane Sarrazin: Sure, sure. Bonjour, tout le monde. Merci, monsieur le Président. Ça sonne un peu comme des noms francophones, donc j'ai pensé peut-être vous remercier pour être ici. Puis aussi, I have to say, I'm really impressed by having companies like yours in Ontario. The majority of the business is in Ontario.

I have to say that, like you—probably not as much as you—I've been participating in some symposiums. Probably, you've been doing it in every province and some other countries, and of course, I think it's a global coordination.

You've talked about the EU AI—whatever. I was in Brussels, and we had a symposium there. I think they're doing great work. I think it will always be a big challenge to balance innovation with public safety, and I think we're going to see that for many years. I think that's the reason going ahead with a bill like this one is important, because, of course, often we see some projects, some bills, some regulations, and we talk about it forever, but it never happens.

Would you agree with us that we need to do it fast, and if we need to adjust after, we'll have the capability to do it?

M. Denis Villeneuve: Définitivement. Merci beaucoup.

What bubbles to the top of my mind is, perfection is the enemy of progress, right? We're significantly behind our American, European and global counterparts, so, yes, get something going. Then, like our colleague said, we can

tweak it as we go along if there need to be changes. The innovation cycles are only getting shorter and shorter, so we have to be able to react and respond accordingly. I do agree.

Mr. Stéphane Sarrazin: Would you like to comment on this?

Ms. Pamela Pelletier: Yes. I do believe that it is essential that we have the framework in place very quickly. The technology is accelerating, like I said earlier, at such an incredible pace, yes, but doing nothing is not an option at this point. This is one of the biggest challenges that we have in the 21st century, but we also have the potential to solve a lot of our challenges, so I do believe strongly that it's critical that we put this in place.

Mr. Stéphane Sarrazin: Would you like to comment?

Ms. Patricia DeGuire: I do, indeed. It is vital that we continue, that we begin, and we've got to start from somewhere. But we've got to begin and get it right. What brought these AI regulations is really telling us that we need to move away from more Industrial Revolution ways of doing things and enter into a more post-modernized way of doing things, and change—a paradigm shift.

We hear a lot about public-private partnerships, and we need more of those. We need to have a collaborative approach in doing the work that we do. At the end of the day, who are we serving? The public. And we must include them. I think the PPP, the three-P approach, would give us greater ability to serve the public, be more nimble and respond quicker than what we are doing right now.

So, yes, go ahead, implement human rights principles. It's a must. We're all human beings; we're born with those rights. Acknowledge them right there, and then we can take them. The thing is, human beings are here, and they must be represented in what we do. But let's act quickly.

The Chair (Mr. Lorne Coe): Thank you very much. That concludes the time available for the government to ask questions.

It does conclude each of your opportunities to present, be asked questions and answer questions for us this afternoon. Thank you so much for being with us.

The committee will now recess until 4 o'clock, and we will hear from the Dais at Toronto Metropolitan University and Victim Services Toronto.

This committee is now in recess until 4 o'clock.

The committee recessed from 1543 to 1601.

VICTIM SERVICES TORONTO

THE DAIS AT TORONTO METROPOLITAN UNIVERSITY

The Chair (Mr. Lorne Coe): I'd like to reconvene the Standing Committee on Justice Policy. We have two new presenters: The Dais at Toronto Metropolitan University and Victim Services Toronto. You will each have seven minutes to make your presentation. Who wants to start? Please state your name for Hansard, and you may begin, please.

Ms. Jasminder Sekhon: Jasminder Sekhon.

The Chair (Mr. Lorne Coe): Thank you for being here. Please start your presentation. If you run over 10 minutes, I will interrupt you.

Ms. Jasminder Sekhon: Okay. Thank you.

Good afternoon members of the committee. Thank you for the opportunity to address you today on Bill 194. My name is Jasminder Sekhon, and I am here to urge this committee to incorporate specific protections within Bill 194 to address the rising harms caused by deepfake technology in our school systems.

Let me begin by telling you a story to illustrate the urgency of this issue. Recently, Victim Services Toronto supported a group of young girls from three different schools. These 11-year-old girls discovered that one of their peers had taken their photos from social media and used a deepfake tool on the Telegram app to alter their images. This app is notoriously known to create and share explicit images that are illegal with privacy and encryption.

In this case, the AI technology stripped these girls not only of their clothing but also of their dignity by creating highly realistic nude images. The images, though fabricated, were so believable that if you did not know they were AI-generated, you would think that they were real.

The effects on these girls were profound. They reported feelings of extreme violation and distress, and when the police investigated, they found that these images had been shown to other students in the school. But the images themselves, because they were deleted, left insufficient evidence for the police to press charges. The laws governing this type of technology haven't caught up with its capabilities, and as a result, the accused walked free.

These girls remained scarred by the incident, carrying real, emotional wounds from an event in which physical harm was not present, yet the impact on their lives was severe. While these images are fake, the impact is the same as if it were real. The violation is real. The humiliation is real. The anxiety is real. And the victimization is real.

Such cases highlight the urgent need for Bill 194 to include specific provisions addressing the emotional and social consequences of digital abuse. The psychological trauma, social isolation and bullying that can result from deepfake harassment are not just incidental; they can be damaging and long-lasting, just like physical abuse.

As legislators, educators and advocates, we have a responsibility to protect our youth, not only from physical harm but also from emotional and psychological harm that can occur within the digital realm. Through Bill 194, Ontario has an opportunity to take meaningful action to prevent further digital abuse within school systems. By equipping school boards with clear and enforceable guidelines, Bill 194 can be a powerful tool in safeguarding our youth.

To address these threats, I recommend the following specific actions:

—immediate response protocols. Schools must have a trauma-informed standardized protocol to respond to deepfake incidents and cases of digital abuse. This includes removing harmful content quickly, providing coun-

selling and mental health support for victims, and taking disciplinary action against perpetrators.

—comprehensive victim support. Addressing this issue is not just about punishing perpetrators, but it's about supporting those who have suffered from the impacts. Our youth deserve counselling services and recovery resources within the school system. Rebuilding a sense of trust and safety for victims should be a priority.

—education on digital literacy and consent. Schools need to offer programs that teach students about the ethical use of technology, the concept of digital consent and the social and legal consequences of the use of deepfake creation and dissemination. This not only deters potential abusers but also empowers victims to make informed, responsible choices. Here, in the city of Toronto, Victim Services offers education through their Teens Ending Abusive Relationships program, which can serve as a model.

And of course, we need monitoring and reporting mechanisms. Schools should have clear systems for identifying and reporting deepfake abuse cases. Trained personnel and sensitive handling of these incidents are essential to ensuring that digital abuse does not go unreported or unaddressed. These recommendations align closely with Ontario's anti-sex trafficking mandates and policies, such as PPM 166, which seeks to keep schools safe from sex trafficking.

By integrating these provisions, Bill 194 could set a new standard for youth-centred cyber security. This bill is a necessary step to safeguard students from unauthorized access to information and exploitation. By clearly defining school-specific protocols to handle digital abuse and deepfake incidents, we can eliminate concerns around enforcement gaps and provide a clear, actionable framework for educators and administrators.

The Ontario Human Rights Commission has raised the issue that without targeted protections, AI-based tools may increase discrimination and harm, particularly in vulnerable groups such as school-aged youth. Integrating expert insights from anti-trafficking and youth protection professionals can greatly enhance Bill 194, making it more than just a digital security measure, but a true line of defence for our youth against new and evolving forms of digital abuse.

The potential of Bill 194 to address digital security across Ontario's public sector is significant. This is an opportunity to address the real, immediate threats that deepfake technology pose to students in our school systems. By mandating trauma-informed response protocols, providing victims support and including digital literacy in school curriculums, Bill 194 can truly protect and empower Ontario's youth in the digital era. These youth deserve to feel safe, respected and valued.

The harms inflicted through deepfake technology, as we have seen, are anything but fictional. They leave lasting scars on the hearts and minds of youth.

Thank you for your time and consideration.

The Chair (Mr. Lorne Coe): Thank you very much for your presentation.

We'll go to André Côté. You have seven minutes, sir. Please start.

Mr. André Côté: Thank you very much. I am with The Dais, which is a think tank and leadership centre at Toronto Metropolitan University, right up the street. We focus on, I would say, applied public policy. Our work focuses at the intersection of innovation and technology, education and democracy. We do a lot of work on tech policy issues, so we're very excited to see the Ontario government and the Legislature advancing this bill. I would say, broadly, our philosophy is trying to balance the growth opportunity with the guardrails side of things, which I think reflects the government's approach as well.

I think, just in starting—and along those lines, I would commend the minister and the government for bringing the bill forward. There is a real need to beef up safeguards around cyber security, AI, digital privacy, with a focus on kids, for sure. I think it's worth noting, also, that a part of what's unique with this approach—we've looked at a lot of the federal legislation and some of the other provinces'. It tends to focus on the private sector, which is very important, but I think there's a big question around public sector cyber security, AI etc. So I think this is a novel and important approach, and one that hopefully other provinces can be looking at as well—so starting there.

1610

We did a submission back when the bill was tabled in—I can't remember, April, May, whenever that was—and so I will speak to a couple of things that we had in our submission and then a few other points or considerations, areas for potential improvement. Just in setting it up, I think starting with the idea of what the bill is supposed to do, to my understanding: on the one hand, strengthen but also set the guardrails for broader public sector use in the areas of cyber security, AI, digital privacy, children's safety.

We're thinking about hospitals, universities, K to 12 schools, children's aid, municipalities, government departments and agencies. This is a super wide mix of organizations—very different context. There will be some similarities, but I think it's important to think about the broad scope of what we're dealing with. Also, the schedule A part at least is more so, I would say, framework legislation that kind of sets the architecture, with the details to be painted in after the fact, which I think is a good approach here, given the breadth of all of this.

So, a first point: It's great to be here with you today. I think further consultation will obviously be critical as this rolls out. I was heartened to hear the minister at the Empire Club this week basically speak to that. This is just the start of the conversation; I think that's great.

A key piece will be who is being consulted. A bunch of great folks are speaking to you today. One thing I saw relatively little of was representation from the broader public sector speaking about their specific issues, their challenges. So I would hope that there can be more discussions with those groups going forward.

Second, given the diversity there, we should be thinking about sectoral approaches rather than broad one-size-fits-

all policies—again, different contexts, risks, threats across the broader public sector, and also widely varying capacity within organizations, from big hospitals to children's aid societies, small colleges etc. The minister, I think, signalled this as well. One thought should be, should these provisions be sequenced as they're rolled out through the next phase—so accommodate them. Some smaller organizations are just going to have a hard time putting some of these things in place.

Think about where to avoid overregulation or red tape here. On the cyber security piece, for example, I think the idea of requiring cyber programs and some standardization is very important, like school boards, for example. Our sense is it's a bit of a Wild West in terms of what they are doing, so there has to be some standardization, some requirements. I think cyber incident reporting is essential. That should totally happen.

Beyond that, I think we should be careful with annual reporting on the progress of your plan etc. etc. At what point do we reach box-checking types of activities? We're talking overburdened organizations already, so think about how to limit that type of thing.

I think the enforcement provisions in the bill could certainly be beefed up. My read—section 13 states, "Failure to comply ... does not affect the validity of any policy, act, regulation, directive, instrument or decision." The next section states that the act is superseded by other acts.

My reading is—and correct me if I'm wrong, but what stops a ministry, an agency, a municipality, a rogue university like mine, from being non-compliant? So I think the act could do a little bit more to beef that up.

One recent example—police services. There have been some major issues recently with police using a service called Clearview AI, which is a facial recognition technology which basically scrapes faces from the Internet. They were doing this without governance in place and without internal controls and in violation of privacy law. So this was investigated and it's now been addressed to some extent, but these are the types of situations that I think we need to be thinking about—so how to beef it up and should there be an independent commissioner or regulator to oversee, like an IPC or another properly-resourced entity for that.

Fifth, there could be a big economic development opportunity here, especially for Ontario's cyber and AI sectors. We have a strong ecosystem of emerging and existing companies—

The Chair (Mr. Lorne Coe): You have 34 seconds, sir.

Mr. André Côté: Okay, perfect.

And we're going to create huge demand through this. So how, basically—and I have some more thoughts, but how, basically, can we support this business to go to Ontario companies as opposed to big, foreign players where the money is just going to trickle across the border?

Last one—coming all the way back to the first point—I think capacity-building tied to the bill is huge—huge capacity gaps across all these sectors. So how do we not just put requirements on but support them in a variety of ways that we can—

The Chair (Mr. Lorne Coe): Sir, your presentation time is concluded.

I didn't mention another group that we have, ISC2. And Pat Bataillon, who is the director of North American advocacy, is joining us virtually, correct? Okay.

Hi, Pat. How are you?

Interjection.

The Chair (Mr. Lorne Coe): You're muted, sir. You've got to get live. Okay. You have seven minutes for your presentation, and that will be followed by questions from the official opposition and then followed by the government members. Start your presentation. Keep it to seven minutes; otherwise, I will need to stop your presentation, okay? Thank you very much, sir.

The Clerk of the Committee (Ms. Thushitha Kobikrishna): His mike is not working.

The Chair (Mr. Lorne Coe): Oh. Your mike is not working.

I'm going to leave it to our Clerk and our audio technician to bring Mr. Bataillon forward.

Committee members, I'm going to start with the questions to the two presenters here, and when we have Mr. Bataillon straightened out with our audio, then we'll bring him back in.

Questions, please, from MPP Glover. When you're ready, sir.

Mr. Chris Glover: First of all, thank you all for being here today. It's great to have these presentations.

I'll begin my questions with Ms. Sekhon. Did I pronounce that correctly?

Ms. Jasminder Sekhon: Yes.

Mr. Chris Glover: Okay. Let's see. You were talking about specific protections, particularly for children, around deepfake technologies in Bill 194. The Information and Privacy Commissioner recommended this afternoon that the legislation be amended to include a declaration of principles similar to another act, and those principles should assert that artificial intelligence should be used in a manner that is valid and reliable, safe, protects privacy, is transparent, accountable and human rights-affirming. Would you agree with that amendment in the bill?

Ms. Jasminder Sekhon: When was this proposed? Just this afternoon?

Mr. Chris Glover: It was proposed by the Information and Privacy Commissioner in their deputation.

Ms. Jasminder Sekhon: Okay, perfect. And that was just today?

Mr. Chris Glover: It was brought forward today in this committee.

1620

Ms. Jasminder Sekhon: Okay. I haven't seen the full deputation so I'm not 100% sure if I can fully speak to that, but that does seem like it is walking along some good lines.

Mr. Chris Glover: Right. What the Information and Privacy Commissioner was asking for is similar things to what you are saying. You talked about this horrific episode

that these young girls experienced with deepfake technology and the shame that they felt and the lack of repercussions for the person who actually committed that crime. This amendment would, in fact, embed in the legislation protections that make sure AI is used in a manner—it would restrict the way that it's used so that it must be valid and reliable, it must be safe, it must protect privacy, it must be transparent so we know when we're responding to AI, it must be accountable and it must be human rights-affirming.

Generally, you want to take another look at it, but generally—

Ms. Jasminder Sekhon: Yes, we're definitely along those same lines.

Mr. Chris Glover: Okay. The other amendment that we're looking at here is to—the European Union Artificial Intelligence Act classifies AI systems in four risk categories to address the varying degrees of potential harm and ethical concerns. There's unacceptable risk, high risk, limited risk and minimal risk. Some things are unacceptable risk: for example, AI being in charge in the deployment of weapons. That would be considered an unacceptable risk. There are other things that are minimal risk or limited risk: AI being used to diagnose, for example, skin ailments. There's a limited risk there. There's some risk, but it's not—you need a human to check with all these things, right? Then there are things—certainly deepfake technology that's used to create pornographic images without the permission of the person whose image is being used, that would be an unacceptable risk.

Would you agree that this kind of risk assessment should be incorporated into this legislation? Or would you be supportive generally, in principle, of this kind of risk assessment?

Ms. Jasminder Sekhon: I definitely believe that the use of deepfake technology does fall within that very high-risk category. I'm not an expert in the field of policy; my expertise really lies in victim support. If that were to enhance support for victims and provide some additional provisions there, then that would be a positive thing for victims.

Mr. Chris Glover: Okay. The other recommendation was around privacy of children, that there's a need to amend and protect children's data, and that children's data should be deemed sensitive with a higher level of protection than for adults. Would you agree in principle with that?

Ms. Jasminder Sekhon: With the principle of that? Yes.

Mr. Chris Glover: Okay, thank you.

I'll ask the same questions of you, Mr. Côté. The first one is embedding in the legislation the principles that AI should be used in a manner that is valid, reliable, safe; protects privacy; is transparent, accountable and human rights-affirming. Would you agree that should be embedded in the legislation?

Mr. André Côté: Sure. I wouldn't disagree with those principles. I think that the challenge with a lot of AI policy-making is there has been a focus on principles as opposed to really specific, prescriptive, enforceable provisions. So I don't see why not, as a starting point, but it's principles-plus. I think that's the key.

Mr. Chris Glover: Thank you. I appreciate that. This is the challenge that we've had with this legislation: The term "transparency" appears once and the term "regulation" appears 52 times. Obviously, in any good AI policy or cyber security policy, transparency should be one of the fundamental principles.

Regulation—the way the Legislature works is the government or the opposition brings forward legislation, it's debated in the House in a public sphere and then that legislation is passed or not passed, but we have a public debate about it. After the legislation is passed, the minister develops regulations to implement that legislation. Most of this piece of legislation just allows the minister to develop regulations behind closed doors without the public debate. This is the challenge—what we're looking for in the opposition is amendments to this bill to incorporate founding principles for AI use so that at least there's a framework that those regulations would have to follow.

Would you be supportive of that, then?

Mr. André Côté: Sure. I'm definitely supportive of inclusion of the principles. I also think that there are some other ways you could potentially add further meat to the bone as you go through.

The one caution I would have—and I totally hear your point on as it moves to that regulatory directive policy-making stage—is it leaves the hands of the legislative body to some extent, although it would be posted on the regulatory registry, I think, right?

Mr. Chris Glover: Yes.

Mr. André Côté: I think the federal government has gotten into a bit of a problem with this as well where, with their AI bill, there was a lot of criticism that, similarly, it was a bit of a framework piece of legislation.

You talked about the European Union, the high-risk approach; the feds adopted this high-impact approach. Why choose a different one? I'm not entirely sure, but it was a similar concept. They were pushed to seek to clarify specifically what might be those higher-impact areas, and the minister came back with a list. The problem was they were being responsive to this demand for more clarity, but it didn't offer an opportunity to properly work through the list in a consultative way either.

So I hear your point, but I don't mind the idea of passing this sort of framework and then working through the bits and pieces after—

The Chair (Mr. Lorne Coe): Thank you, sir. That completes the first round of questions from the official opposition.

MPP Riddell, please. When you're ready, sir.

Mr. Brian Riddell: My question is to you, sir. As experts in the intersection of technology, innovation and public policy, what type of high-risk AI use cases do you believe should be the primary focus for the regulatory model introduced in Bill 194?

Mr. André Côté: I think AI deepfakes would be high on the list, for sure, and particularly where there's this intersection—

Mr. Brian Riddell: That's where I'm taking this question next, but I wanted to get your thoughts.

Mr. André Côté: I know other hotly debated areas are areas like, for example, real-time facial recognition technology used by law enforcement; that was hotly debated in Europe, so I think there's some sort of category of those. They also looked at social scoring, like with what the Chinese Communist Party has put in place.

So it's that category of, I think, extremely and highly invasive, or dangerous, types of applications.

Mr. Brian Riddell: So, some of my background: I used to teach Creative Cloud and Adobe Photoshop, and there's software that's much easier to use now to replicate somebody's face onto another person's body or the other way around.

But how would you answer that question, if I asked you? I can repeat it if you wish.

Ms. Jasminder Sekhon: If you could, please.

Mr. Brian Riddell: Let me ask you something else here. What requirements, to you, should be prioritized for artificial intelligence guardrails for the private and public sector—I'm going to go with just the public sector organizations? What do you feel?

Ms. Jasminder Sekhon: I think the regulation, especially around deepfake and AI, should particularly be, when we're thinking about the public sector, around school systems as well as children's aid societies.

Mr. Brian Riddell: Yes. I think children should be a main focus just because they're so vulnerable, and the examples that you gave are heart-wrenching. I think it's absolutely horrible that there are people in the world today that will do stuff like that, and I commend you on everything that you have done to help it.

But if I ask both of you, do you both support this bill?

Ms. Jasminder Sekhon: Yes. I definitely believe that it is a great first step, and of course, there are other pieces where it can be enhanced, absolutely. But I definitely think that it's along the right direction.

Mr. Brian Riddell: Sir?

Mr. André Côté: Yes, I strongly agree. I think the devil will be in the details on some of the elements, but, broadly speaking, I strongly support it.

Mr. Brian Riddell: As far as the minister's ability to make changes as we go along—and I think the reason behind that is because AI just changed from a minute ago to now. We need to have that facility to go in there and make those changes as required.

What are your thoughts on that?

Mr. André Côté: I mean, I agree. I think that's partly why I don't mind the framework approach because it gives a little more flexibility in updating over time, whereas if you seek to hard-code things in legislation on the front end, it just makes it more challenging to change down the road. Plus, these bills are just so complicated, right? With these new technologies, can you also have an informed debate about a bill where you're seeking to hard-code all the very specific components?

1630

I think you want a balance, right? There are certain aspects that you should seek to properly clarify in the legislation. Hopefully, that answers it.

Mr. Brian Riddell: I think it's needed, from my point of view.

Now I will turn it over to MPP Saunderson.

The Chair (Mr. Lorne Coe): MPP Saunderson, please, when you're ready.

Mr. Brian Saunderson: Thank you, both of you, for appearing here today.

Ms. Sekhon, I have a question for you. You were talking about a mandatory reporting requirement, and it's something that's certainly being contemplated in the legislation. Can you give me some thoughts on how you think that would best be implemented, particularly in the egregious situations you've outlined for us?

Ms. Jasminder Sekhon: Absolutely. When I'm speaking about reporting mechanisms, I'm really focusing on what we can do for schools, and I think that there are already actually reporting mechanisms in place, pre-existing at schools, around sexual violence policies and human trafficking policies, especially if those images are being altered and then sold for a profit. I believe that we can build on and work with schools that already have these pre-existing policies and structures in place to help bolster those and make sure that AI deepfake technology is included within that.

Mr. Brian Saunderson: How much time do we have, Mr. Chair?

The Chair (Mr. Lorne Coe): You have two minutes and 25 seconds, so two more questions.

Mr. Brian Saunderson: Two more questions?

The Chair (Mr. Lorne Coe): There you go.

Mr. Brian Saunderson: Do you want to go for it? Go ahead.

The Chair (Mr. Lorne Coe): MPP Sarrazin, please.

Mr. Stéphane Sarrazin: My question is for André. You were talking about the economic opportunity for companies in the province of Ontario. I guess you didn't have enough time. Maybe you can elaborate on that.

Mr. André Côté: Sure. I think this could use more thought, but one thing I liked that the ministry has already done is develop a vendor-of-record for cyber companies, basically as sort of a support service to broader public sector organizations.

Should there be an effort to do something similar, but through kind of a buy-Ontario lens, to be crass about it? Honestly, we're in a bit more of a protectionist world now anyway. Would it be possible to do that?

Essentially, you would be able to vet a set of Canadian or Ontario companies. You wouldn't force broader public sector players to use them, but you could make clear that these are vetted companies that can provide these services and that you should feel comfortable contracting with—something like that.

Mr. Stéphane Sarrazin: All right. Does anybody have more questions?

The Chair (Mr. Lorne Coe): You have one minute and 30 seconds.

Mr. Brian Riddell: I will ask you, sir. Can you give your thoughts on how any future regulations could take into account protections for victims of crimes and tragedies at a university level? I think it would be quite large, the potential.

Mr. André Côté: Victims? Honestly, that's not an area that I could speak to with any confidence about, so I don't just want to make something up.

Mr. Brian Saunderson: So I'll go over to you.

Ms. Jasminder Sekhon: Can you repeat your question?

Mr. Brian Riddell: Can you give us your thoughts on how any future regulations could take into account protections for victims of crimes and tragedies?

Ms. Jasminder Sekhon: Absolutely. I definitely think that in the same way that high schools and elementary schools have systems in place, when it comes to sexual violence policies and policies along those lines—universities already have these in place. But I do think that they have not caught up yet to the changing times and they have not caught up with AI technology at all. And so, what we continue to see is—

The Chair (Mr. Lorne Coe): Thank you very much for that response. The time for government questions has concluded.

We're back for the second round to the member of the official opposition. MPP Glover, please, sir, when you're ready.

Mr. Chris Glover: I'll let you finish your thought there, Ms. Sekhon.

Ms. Jasminder Sekhon: It's okay.

Mr. Chris Glover: Yes? Okay.

Let me explain to both of you one of the challenges we have in the opposition with this bill. The bill actually states that one of the fundamental principles of good AI policy development is transparency.

Normally, when a bill goes through this Legislature, it goes through two readings. Then it comes to committee and then the committee can actually travel with the bill around the province; have consultations with different people, agencies and whoever wants to come and speak to get input; and then incorporate those into amendments in the bill. That process was not followed in this case. What happened was the government introduced the bill, they recessed for the summer and the minister had private consultations all summer without the committee, without other opposition parties being able to be present, so there was no transparency in the development of this bill through the summer.

The other challenge is that this bill, as I mentioned earlier—there is very little meat in this bill. It's almost all empowering the minister to create regulations behind closed doors, so one of our big concerns with this bill is that there are not even foundational principles of what is good use of AI.

I know the government side was asking if you support this bill. I understand that you would support an amendment to specify what is an appropriate use of AI; that AI should be used in a manner—and I mentioned human rights, protecting privacy, etc. Do you support this bill if that foundational principle statement is not in the bill?

Mr. André Côté: I'm happy to take a run at this. I'm just not aware enough of the legislative process and how that unfolded to really comment on that.

Mr. Chris Glover: Let me pick up on something that you said earlier, then. You mentioned that you want to see—it's really the nuts and bolts; the proof is in the pudding with this. And you would like to see a transparent process: Like, sure, it's fine to have a broad bill and it's good that we are actually having this discussion, but we really need to have public consultation in the further development of regulations that are actually going to be the nuts and bolts of this bill.

The way it currently stands, those consultations will not necessarily take place. They could take place behind closed doors. There is no requirement for public consultation. What we're asking for in the opposition is that the bill be amended so, at least, we have foundational principles that those regulations have to follow. Otherwise those regulations—there is no real restriction on what they could be and there is no public oversight of who is in the room recommending those regulations.

Would you support this bill if it doesn't include foundational principles about how AI should be used or should be developed?

Mr. André Côté: I mean, honestly, I would. I do think the principles could be a valuable addition. In a majority government especially—and it has gone the other way in the past—the government has the ability to advance these things. I think I would say to the minister that if you want to make this bill as effective as possible, it will be in your best interest to consult publicly, but also I think really to consult with these broader public sector entities that are going to be most affected, that these requirements are going to be imposed upon.

And I would say you're right: It's quite broad in terms of the AI provisions. But I would say ideas like requiring transparency in the use of AI are important. How that works will have to be sorted out; that will be an important detail.

I also think a requirement around putting in place accountability and risk assessment frameworks will be very important. A little bit of standardization across the broader public sector—what those look like is still to be determined. But I would just say I like the broad set of provisions, and I hope that the minister and the government properly consult on the next phase.

Mr. Chris Glover: Okay, thank you.

I'll pass that question over to you, Ms. Sekhon.

Ms. Jasminder Sekhon: Yes, I definitely think that was very well said by my fellow deputant here as well, just around ensuring that—I'm also not as familiar with the legislative process, but with the understanding that, of course, consulting public entities, including entities that

you may not expect, such as victim services, can really help bolster something along these lines.

In general, I definitely do think that this provides the foundation to provide additional oversight, and so I would definitely be in support as well.

Mr. Chris Glover: In support of that amendment?

Ms. Jasminder Sekhon: I would be in support of the bill in general to pass. But of course that would definitely help bolster the bill as well.

Mr. Chris Glover: And you want to see transparency and open public consultation in the further development of this bill?

Ms. Jasminder Sekhon: I definitely believe that consulting with outside organizations would help make the bill the best it could be.

Mr. Chris Glover: Okay, thank you. Those are all my questions.

The Chair (Mr. Lorne Coe): You have one minute and 51 seconds.

Mr. Chris Glover: I'll pass.

1640

The Chair (Mr. Lorne Coe): You're done?

Mr. Chris Glover: Yes.

The Chair (Mr. Lorne Coe): All right.

Back to the government side, please: MPP Riddell.

Mr. Brian Riddell: Our government is committed to supporting measures that better safeguard children's privacy in today's increasingly digital world. That really sounds a bell with me because I believe children are so vulnerable and they need to be protected.

So I'll ask each of you, how can the government and community partners improve collaboration to strengthen cyber resiliency and maturity?

Ms. Jasminder Sekhon: In general, there are a couple of major things that this bill already addresses, around increased transparency; more content moderation, as well, which is required, especially when it comes to youth; also, with the enhancement of consumer privacy and some more information around that, through this bill—that has definitely been bolstered, and so I think that's a positive thing.

When it comes to youth and how we can provide additional supports and resources for them, as I mentioned, I believe the education piece is quite key. I also feel that once youth experience any of these forms of violence, there need to be solid reporting mechanisms that are in place in order to provide support to those young people as well.

Mr. André Côté: I would say a couple of things. Firstly, the bill seeks to build cyber resilience across the broader public sector, including school boards, including in the K-12 system, where we know there have been cyber attacks. Generally, these are institutions that are just not that well-equipped for this. So, firstly, in terms of protecting kids, having those institutions beef up their supports, where they are the holders of a lot of valuable children's PI, basically—I think that's step 1.

I think step 2—and where this is so complicated is, there's an important intersection with other legislative action. Federal Bill C-63, online harms—very focused on some of the major areas of harm around kids, is where that bill would seek to be the toughest. Regulating social media is not something that is really in scope for this. So I think there's a key challenge for legislators in terms of, what's the intersection to make sure that we're protecting kids in alignment with—and we'll see if that federal bill passes.

The last thing I would say is definitely the digital literacy development—we're doing sort of a pilot thing right now with the Ministry of Education where we're building these voluntary lesson plans for educators, and one of them is on deepfakes; another is on how to understand news on social media. They're sort of supplemental to the curriculum, but educators can use them to start to teach their kids in grades 6, 7, 8, 9 about these things. So we think that's positive, but it's just the tip of the iceberg. We need to think about this in a much more holistic way.

Mr. Brian Riddell: Even if I wasn't sitting here right now and I heard of this bill, I'd be very supportive of it. Children are our future, and we have to give them the best possible ability to see some of these deepfakes and to prevent some of the horrible things that you stated earlier.

Should this bill pass, the Ontario government would collaborate with school boards, guardians, parents, as well as groups overseeing children in provincial settings, to ensure the right protections are introduced without affecting the quality of education or care. The province would also consult with children's experts on setting safeguards to ensure age-appropriate use of third-party applications in schools and children's aid societies.

The province will continue consulting with key public sector stakeholders, including Indigenous partners, academia, technology and AI experts, and the Ontario Human Rights Commission and Information and Privacy Commissioner of Ontario. In saying that, we are going to have consultations in the future to do the right things for the people of Ontario.

I'll do a time check.

The Chair (Mr. Lorne Coe): You have three minutes and one second.

Mr. Brian Riddell: I'll pass it over to MPP Dixon.

The Chair (Mr. Lorne Coe): MPP Dixon, you have a question?

Ms. Jess Dixon: I have, I suppose, a question-statement, but I was listening, ma'am, to what you said with a great deal of interest. I know Victim Services Toronto brings so much passion to that.

I did want to let you know that the idea of, particularly, deepfakes, the response to deepfakes and that type of thing, has been also extensively covered in the IPV/sexual-violence committee that's been ongoing. We've had a very deep dive into that, and I think a lot of really actionable recommendations coming out of that, so we are very, very aware of it.

Given that we only have a couple of minutes left, I just wonder if you have an idea, as far as—if you can expand a little bit more on what you said about CAS? You talked about the boards and CAS.

Ms. Jasminder Sekhon: Yes, for sure. We have actually seen some exploitation within families, as well, of young

children, in terms of family members creating and disseminating some of these photos as well. So I think providing some additional supports and resources for CAS workers and agencies, as well as just some clarity around that, would be helpful, because I do think one of the challenges here is that perhaps a child may not be at imminent risk of physical harm, or there's no physical or sexual harm that's taking place, but there is a real psychological harm that's taking place. That becomes one of the challenges, as well, that we definitely think would be very valuable to address.

Ms. Jess Dixon: Okay. Thank you so much.

The Chair (Mr. Lorne Coe): You have one minute and four seconds.

Mr. Brian Riddell: We have no further questions.

The Chair (Mr. Lorne Coe): You're done? All right. Thank you.

Mr. Bataillon hasn't been able to join us, so consequently we will not be hearing from him nor will we have the ability to ask questions. That is consistent with the standing orders originated for the committee meeting today, as well as tomorrow.

To that, this concludes our public hearings on Bill 194 for today. As a reminder, the deadline for written submissions is 6 p.m. on Friday, November 15, 2024. The deadline for filing amendments to the bill is 5 p.m. on Tuesday, November 19, 2024.

The committee is now adjourned until 10 a.m. on Friday, November 15, 2024. I think it's committee room 2.

The committee adjourned at 1648.

STANDING COMMITTEE ON JUSTICE POLICY

Chair / Président
Mr. Lorne Coe (Whitby PC)

Vice-Chair / Vice-Président
Mr. Sol Mamakwa (Kiiwetinoong ND)

Mr. Will Bouma (Brantford–Brant PC)
Mr. Lorne Coe (Whitby PC)
Ms. Jess Dixon (Kitchener South–Hespeler / Kitchener-Sud–Hespeler PC)
Mr. Sol Mamakwa (Kiiwetinoong ND)
Mr. Brian Riddell (Cambridge PC)
Mr. Stéphane Sarrazin (Glengarry–Prescott–Russell PC)
Mr. Brian Saunderson (Simcoe–Grey PC)
Ms. Effie J. Triantafilopoulos (Oakville North–Burlington / Oakville-Nord–Burlington PC)
MPP Kristyn Wong-Tam (Toronto Centre / Toronto-Centre ND)

Substitutions / Membres remplaçants
Mr. Aris Babikian (Scarborough–Agincourt PC)
Mr. Chris Glover (Spadina–Fort York ND)

Clerk / Greffière
Ms. Thushitha Kobikrishna

Staff / Personnel
Ms. Heather Conklin, research officer,
Research Services
Mr. Andrew McNaught, research officer,
Research Services