Legislative
Assembly
of Ontario

Assemblée
législative
de l’Ontario

Official Report of Debates (Hansard)

JP-55

Standing Committee on Justice Policy

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

1st Session
43rd Parliament

Friday 15 November 2024

Chair: Lorne Coe
Clerk: Thushitha Kobikrishna

Journal des débats (Hansard)

JP-55

Comité permanent de la justice

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

1re session
43e législature

Vendredi 15 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

Friday 15 November 2024

LEGISLATIVE ASSEMBLY OF ONTARIO

ASSEMBLÉE LÉGISLATIVE DE L'ONTARIO

STANDING COMMITTEE ON JUSTICE POLICY

COMITÉ PERMANENT DE LA JUSTICE

Friday 15 November 2024

Vendredi 15 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. Welcome to the Standing Committee on Justice Policy. I call this meeting of the committee to order.

We are meeting today to 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, committee members, the deadline for written submissions is 6 p.m. today, November 15, 2024. The deadline for filing amendments to the bill is 5 p.m. on Tuesday, November 19, 2024. Are there any questions before we begin our public hearings? Seeing none, I will just turn to page 2 of my commentary.

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 have heard from all three presenters, the remaining 39 minutes of the time slot will be for questions from members of the committee. Remember, 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 members of the committee.

ROGERS CYBERSECURE CATALYST

ENGINEERS FOR THE PROFESSION

LAW COMMISSION OF ONTARIO

The Chair (Mr. Lorne Coe): I now would like to call forward Rogers Cybersecure Catalyst, Toronto Metropolitan University. I believe you're at the table, is that correct?

Mr. Charles Finlay: Yes, sir.

The Chair (Mr. Lorne Coe): All right. If you could please identify yourself for the purpose of Hansard, which is the official recording service of the Ontario Legislature.

Mr. Charles Finlay: My name is Charles Finlay. I am the executive director of the Rogers Cybersecure Catalyst at Toronto Metropolitan University.

The Chair (Mr. Lorne Coe): Well, thank you, sir, and welcome to the committee. You have seven minutes for your presentation. If you go over seven minutes, I'm going to interrupt you and I'll move to the next presenter. You can start your presentation, please, when you're ready.

Mr. Charles Finlay: Excellent. Thank you very much, Chair and members of the committee. As I mentioned, my name is Charles Finlay, I'm the founding executive director of the Rogers Cybersecure Catalyst at Toronto Metropolitan University. The catalyst is one of Canada's most active university-based hubs for cyber security training, commercial acceleration, research collaboration, public education and policy development. We are a part of Toronto Metropolitan University and we have our headquarters in Brampton, Ontario. The catalyst is strictly non-partisan. We enjoy productive and important partnerships with private sector and public sector partners of all kinds.

I am here to offer perspective on Ontario Bill 194, in particular the section on cyber security, which are sections 2 through 4. Let me say that I think this legislation is important and timely. I urge its passage into law soon. I also hope that its regulations will be issued quickly.

I think it is important at the outset to offer some context for this legislation. Bluntly, the cyber-security-threat environment in Canada and in Ontario is very serious. A wide array of threat actors, including nation-states, criminal mischief-makers and combinations of these varieties, are undertaking an array of destructive cyber attacks against targets in Ontario, literally all the time. Taking the public sector entities to which Bill 194 will apply, the cyber security situation is dangerous. We have seen, in Ontario, significant cyber security attacks against hospitals, including the sick children's hospital in December 2022 and the attack against hospitals in southwestern Ontario in October 2023. We have seen major attacks against school boards, including against the Toronto District School Board in June of this year, York Region District School Board in November 2023, Waterloo Region District School Board in July 2022 and Peel District School Board in January 2021.

Municipalities are coming under increased pressure from cyber attacks as well. The city of Hamilton suffered a devastating attack earlier this year, as did Huntsville. St. Marys suffered a major attack in 2022, and Stratford suffered a serious ransomware attack in 2019.

The attack on Stratford, Ontario, was sufficiently traumatic for that community that Stratford's then-mayor, Dan Mathieson, became a noted public advocate for municipal preparation for cyber attacks and is now a senior adviser in my organization, advising municipalities on how to prepare for cyber attacks.

Since 2016, children's aid societies have come under attack. The children's aid societies of Oxford, Algoma; Lanark, and Leeds and Grenville have all suffered cyber attacks of varying degrees.

This cyber-security-threat environment in Ontario is by no means unique. Globally, cyber attacks by groups based in authoritarian nations are on the rise against targets in the democratic West. The motives behind these attacks are often a mixture of ideological and financial objectives. The ideological objective is to destabilize important institutions, test cyber defences and steal data and intellectual property. The financial objective is to win a ransom from the victim or to earn money from the sale of stolen data.

Whatever the objective, the outcome of these attacks is often devastating for the public sector institution that is targeted and, perhaps most importantly, for the citizens of our province, who will go without critical health care or educational services, will have their municipality disabled, sometimes for months, and could have their personal information sold to the highest bidder.

Though of course certain details will be indicated in the regulations, proposed Bill 194 will do, I think, several very important things. Sections 2(1)(a) and (b), together with sections 2(2)(a) and (d), may require public sector entities to develop and implement programs for ensuring cyber security, which could include the indication of specific roles and responsibilities for individuals within organizations and response and recovery measures for cyber security incidents.

In other words, these sections may require the institutions to which they apply to have a plan in place, with roles of specific individuals set out. We think this is vital. Having a plan in advance of a cyber attack is often the most important factor in how successfully an institution will recover from an attack. In a best-case scenario, these plans would be practised by the required personnel so that there is no guesswork necessary when the crisis happens.

Looking at section 2(2)(c), it may require that a public sector entity have education and awareness measures in place respecting cyber security. This is critical as well. It is well understood in the cyber security ecosystem that a majority of cyber attacks on organizations of all kinds are facilitated in part by employees who make mistakes in how they deal with emails which are sent to them or who have weak passwords or who do not enable two-factor authentication. Educating employees about cyber security risks so that they do not, for example, click on links in emails from untrusted senders, is extremely important.

Finally, section 2(2)(b), the requirement to report progress, is important. Transparency is lacking in cyber security across parts of the public and private sectors. It is difficult to tell how advanced organizations are in their cyber security planning or in their implementation of incident response plans. Having public sector organizations in Ontario report to the government on their progress will keep these organizations accountable and will drive adoption quickly, which is essential in this threat environment.

Finally, I would note that though this legislation leaves many details to regulation, I think that this is better in this case than the alternative. The cyber-security-threat environment is moving quickly. Artificial intelligence, quantum computing threats, in particular, are changing how we respond to cyber threats.

The Chair (Mr. Lorne Coe): Thank you, Mr. Finlay. Your presentation is concluded.

I'm now going to move to Engineers for the Profession, please. Are you there?

Mr. George Comrie: Yes.

The Chair (Mr. Lorne Coe): Fine. Sir, you have seven minutes for your presentation. I need your name and affiliation with the engineers. You can start your presentation after you have identified yourself, please, sir.

Mr. George Comrie: My name is George Comrie, and I'm the vice-president of an organization called E4Pinc, Engineers for the Profession Inc.

1010

The Chair (Mr. Lorne Coe): You have seven minutes, sir. Thank you.

Mr. George Comrie: Good morning, Mr. Chair, members of the committee and ladies and gentlemen. Thanks for hearing us today. As I said, my name is George Comrie, and with me is Peter DeVita. We belong to an organization called Engineers for the Profession, or E4Pinc for short, which advocates for the full utilization of Canada's applied science and engineering professions in the public interest. I would point out that we are a not-for-profit organization. We're not here to sell you anything, just to give advice.

Both Peter and I are past presidents of the association of Professional Engineers Ontario, which, as you probably know, is, by statute, the regulator of Ontario's engineering profession. Both of us have taught and practised software and systems engineering for over 40 years and have domain expertise in the subject matter of today's hearing. The bulk of my practice has involved the development and implementation of mission-critical or safety-critical systems, like operational-police-information systems and systems to control trains and nuclear power plants. These are systems that have to be reliable, continuously available and secure. I was doing that well before the Internet as we know it today existed—and all of its associated problems. I also, by the way, happen to be mayor of a small municipality in west Parry Sound district, so I have the perspective of a public sector agency to which Bill 194 will apply.

Let me begin with a question to you: Here in Ontario, when you enter a modern building or cross a bridge, do you worry that it will collapse and kill you? When you drink water from your tap, do you worry that you will get sick and die? Well, I don't worry. That's because I know someone competent has designed and overseen construction and implementation of our critical physical infrastructure, namely a licensed professional engineer. I know that by law, only a licensed professional engineer is allowed to do that work.

We're here today to talk about the subject matter of Bill 194: cyber security, artificial intelligence, quantum computing and so on. Which begs the question: Why are we experiencing so much trouble with this segment of our critical infrastructure? Why are we hearing daily about the insecurity of our networks and systems, about criminals and rogue state actors stealing our data and our money, extorting ransoms, crippling our public and private systems and so on, as the previous speaker has presented.

I believe that's because, still today, there are few, if any, regulations or professional standards for how this kind of work has to be done, and anyone is allowed to do it. When it comes to software engineering, cyber security and the public Internet, we're still in the Wild West. This needs to change if we're going to regain trust in our information infrastructure.

In fact, the situation is worse than most people realize. Cyber incidents are increasing in number and sophistication faster than our ability to prevent, detect and deal with them. I don't have time to go into much detail on this today, but you can find examples and some statistics in the handout that we've provided. I'm sorry to have to tell you that Canada, and that includes Ontario, is, I believe, falling behind other nations in addressing this crisis. That's why E4Pinc has initiated an online petition to the Parliament of Canada, calling on the Prime Minister to convene a first ministers' conference to come up with a national strategy to combat cyber insecurity—you can find the details on the last page of our handout. I hope that you will sign it and encourage your friends and colleagues to do the same.

We—"we" being Canada—desperately need a cohesive and comprehensive national strategy to safeguard our citizens and all sectors of our critical infrastructure.

As to our reaction to Bill 194: In a nutshell, we agree that public agencies should be held accountable for the security and privacy of their systems, and Bill 194 does provide a legal framework for that. But the devil is in the details, which in this case are in regulations yet to be drafted. We do have to question how regulations can ever keep up with the rapid advances in information technology, particularly in areas like AI and quantum computing.

But there is an even bigger problem: Canada is short a large number of people with the skills necessary to address our cyber insecurity. The latest figure we have suggests that number is around 40,000 for Canada, and in the US, it's around 250,000. To make matters worse, there's little consensus around what specific competencies are required for the different roles and how to measure them.

Our group has worked to define core bodies of knowledge for network engineering practice, but our educational institutions have generally been slow to introduce programs in this area. I say that with full respect to the previous speaker, because his educational institution has in fact done that.

We see this lack of competent, trustworthy individuals as the biggest obstacle to success in dealing with the problem. One thing is certain: We can't legislate a solution without at the same time dealing with a skills shortage. If the government fails to ensure the availability of necessary human and technical resources—

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

We're going to move to the Law Commission of Ontario. The people speaking, please introduce yourself for the record of Hansard.

Mr. Nye Thomas: Sure. My name is Nye Thomas, I'm executive director of the law commission, and my colleague is Susie Lindsay, who is counsel at the law commission.

The Chair (Mr. Lorne Coe): All right, sir. You have seven minutes for your presentation.

Mr. Nye Thomas: Thank you. I'd like to thank the committee for the opportunity to talk about Bill 194. As you may know, the Law Commission of Ontario is an independent legal research institution located at Osgoode Hall Law School. We have been working on the issue of AI regulation and legislation for several years now, and our submission includes a lot of our reports. I'm not going to go into that detail.

What I want to say is to really focus on three essential comments on the concept of trustworthy AI, and some of the ways we think that Bill 194 can be improved.

My first point is that AI regulation, in particular public sector AI regulation, is not a new field. We now have a lot of experience in a lot of jurisdictions tackling the very issues that we are confronting in Ontario. There has been a lot of trial and error; it's not a blank slate like it was three or four years ago, where people were throwing up their hands and saying, "I don't know what to do about this mysterious technology." We have experience, and what we have learned from this experience in other jurisdictions is that there is a package of legislative reforms, legislative principles, often described as being "trustworthy AI," that is appropriate to govern public sector AI systems. These include things like disclosure, public AI registries, protecting privacy, protecting human rights, identifying and mitigating the highest-risk AI systems, impact assessments, explainability etc. So we know what to do; this is not a mystery.

Bill 194 addresses many of these areas, but it is incomplete, and our recommendations would go a long way, we believe, to establishing an appropriate safety net to govern the use of AI systems in Ontario. That's point number one.

Point number 2 is that an important gap in Bill 194 is that it does not cover criminal AI systems used in a criminal justice system. We know from experience—in other jurisdictions, again—that technologies like facial recognition, surveillance biometrics, surveillance and predictive policing, bail and sentencing algorithms are, in fact, the highest-risk AI systems. They are the riskiest because they are the most intrusive, and they are the riskiest because they touch on fundamental human rights: the right to liberty, the right to due process, equality of rights.

In many jurisdictions—indeed, most that I'm aware of—these risks are incorporated in one way, shape or form in their AI regulation. Bill 194 does not cover AI in the criminal justice system, and we believe that is an important gap that needs to be filled, again, to establish these guardrails and safety nets for beneficial AI in Ontario.

1020

The third point I want to make is that we actually know what's going to happen if we don't regulate AI effectively—again, looking at different jurisdictions. We have experience. We can learn from the hard lessons that other communities and other jurisdictions have experienced.

We know there's a risk of privacy loss. We know there's risk to human rights. We know there's surveillance risk. We know there's a risk of compounding the overrepresentation of racialized communities in the criminal justice system. We know these things can happen to poorly regulated AI systems, and in our view, we believe that the province of Ontario should learn from these experiences, learn from these lessons, and build appropriate safeguards into 194.

I'm now going turn to my colleague Susie Lindsay who is going to make some comments on some of our specific recommendations.

Ms. Susie Lindsay: Hello. Thank you for having us here today. The law commission, in our submission, makes 10 recommendations. The first seven are recommendations for amendments to the specific wording of Bill 194, and the last three are suggestions for promises the province can make to the people of Ontario. We see the purpose of Bill 194 as the government wanting to harness the benefits of AI and minimize the harms that we know that it can cause.

I'll just talk about a few of our recommendations. The first one is we think there should be a commitment to the trustworthy AI principles that Nye just talked about enshrined in the legislation. AI principles around the world are fairly aligned: the EU, the US, Ontario. In Ontario's Trustworthy AI Framework that you developed a couple of years ago, there are fantastic principles in there, and enshrining them in the legislation aligns you with other jurisdictions, because that's what we can all sort of agree on. Once we get into the details, yes, people differ as to how we should actually operationalize those principles, but the principles we can agree on. The preamble is an interpretive guide. It gives people a guide for how they should interpret this legislation.

The second thing is, to build on what Nye said, our submission is that this bill should apply to all public entities that deploy AI, specifically high-risk, but the entire public sector, with the idea—and the next point is—that there's a risk regulatory model here. Not all AI is the same, and not all AI uses should be treated the same. The province should have risk categories. These risk categories should be transparent—people should know what they are—and they should be consistent. AI that's in a high-risk category should have more rules on it. For AI we're not worried about, we don't need to worry; we don't need to apply rules to it.

There should be no AI in secret. Those are the words right from the provincial trustworthy AI framework. We think that all AI systems should be listed in a registry, and every person—if there's a decision that's made about somebody, they should be informed if that decision was made by AI.

But when you get into more risky AI, then more stuff has to be disclosed, and we have greater obligations. And again, once we get into these riskier AI systems, we need to have more accountability measures: requirements for monitoring, evaluating, reporting; third-party independent audits; explainability requirements; metrics testing; debiasing techniques; employee training; data governance and data quality; consultations. These are all things that we know—these are all guardrails that can help ensure that the harm AI systems can cause is minimized.

To build on what Nye said, there are risks, but there are also known harms. We've seen it in other jurisdictions. We think Ontario is in a great position to do this really well and not make the mistakes that our friends have made in other places.

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

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

Mr. Chris Glover: Thank you to all the presenters for being here and taking the time. I really appreciate your presentations.

I'm going to start with the law commission. Mr. Thomas and Ms. Lindsay, thank you for your deputation here today. You were talking about how there are places where AI systems just shouldn't be used, and you were talking about the criminal justice system. We've had the example of the Clearview used by police forces. Are you familiar with that example? Could you explain that a little bit for the members of the committee?

Mr. Nye Thomas: Sure. In AI regulation, there's a lot of conversation about what systems should be prohibited—flat-out prohibited. Often, those arise in the criminal justice system.

The most common prohibition around the world—I'm going to get to Clearview—is around what's called real-time biometric surveillance, so real-time facial recognition surveillance: CCTV cameras outside of Queen's Park or Nathan Phillips Square or wherever monitoring people as they go by. That kind of Big Brother surveillance is typically banned in a lot of jurisdictions. There are some law enforcement exceptions to that—bright-line prohibition, catching known fugitives, terrorism, kidnapping, things like that—which are reasonable. So what we recommend is that there, in fact, be prohibitions like that.

The Clearview example is a little more technical. It has to do with some police services using this technology, Clearview, to compare suspects to images on the Internet, which created very significant privacy risks. What the privacy commissioner said was that that kind of Internet scraping, that kind of wide net-casting of everyone on the

Internet, is just not appropriate, and there have to be guardrails around the police use of facial recognition technology as an investigative tool. We support those guardrails.

Mr. Chris Glover: Thank you. First of all, there's an incredible risk to human rights, risk of surveillance and risk of discrimination with the use of AI, and you made a couple of recommendations. You recommended that AI principles be enshrined in this legislation and not just be left to regulation. The IPC recommended that these following principles be inserted into the legislation: that AI should be used in a manner that is valid and reliable, safe, protects privacy, transparent, accountable and human-rights-affirming. Would you agree with having those embedded in the legislation?

Mr. Nye Thomas: Yes.

Mr. Chris Glover: Okay. Let me just ask the others quickly, if I could. George, we'll start with you. Would you also agree that those principles should be enshrined in this legislation?

Mr. George Comrie: Yes, I think so.

Mr. Chris Glover: Okay. And Mister—sorry, I've lost your name here.

Mr. Charles Finlay: Mr. Finlay.

Mr. Chris Glover: Finlay, yes.

Mr. Charles Finlay: In respect to the AI provision, potentially, yes.

Mr. Chris Glover: Thank you for that.

The other recommendation from the IPC was that—and you spoke to it, the law society; you talked about classifying the risk of AI. The EU Artificial Intelligence Act classifies AI systems into four risk categories: minimal risk, limited risk, high risk and unacceptable risk. Would you agree with having those risk categories be inserted into this legislation?

Ms. Susie Lindsay: I think there needs to be risk categories. In an ideal world, the government will have consultations with people as to what is best for Ontario. There are some people who have suggested to me that five categories are correct. The EU four categories is another option. The one thing we don't really support is the binary two categories of high impact and not high impact. It's a bit too blunt.

Mr. Chris Glover: I see. Okay. Thank you for that.

Considering where AI is right now and where cyber security is right now, I think this is probably the most important piece of legislation that we're going to pass in this session—I see some nods over there that this is probably true. It will have the greatest impact on the future.

One of our concerns in the opposition is that there is very little meat in this legislation. Everything is left to regulation. When I've been consulting with people, one of the principles of good AI and cyber security legislation or policy-making is that it should be transparent and that there should at least be principles enshrined so that we know what the regulations are being built on, so the regulations can't just be at the whim of a minister without some sort of guardrails.

Would you agree that there should be guardrails inserted in this, and that the legislation, as it stands, just empowers the minister to create policy without a public debate?

Mr. Charles Finlay: Respectfully, I think not. One of the significant features of the current threat environment in respect of cyber security is how quickly it is moving, how quickly the technologies are changing, how quickly the threat actors are innovating. In our view, the regulations may be changed more quickly than enacting legislation. In our view, having the force of this legislation carried in the regulations in respect of the cyber security section is appropriate in the circumstances.

1030

Mr. Chris Glover: I agree with you: Cyber security is changing. AI is changing. This legislation—there needs to be a nimble response from the government that the legislative process is not able to do quickly enough. So we do need to be able to develop regulation, and I fully agree with you.

The question is: Should we have some guardrails, some guidelines on what those regulations should be about? I gave the example earlier about the IPC, the Information and Privacy Commissioner's recommendations on the definition of appropriate uses of AI.

Let me ask you this again: Would you support the AI having risk categories of AI inserted in the legislation?

Mr. Charles Finlay: To me?

Mr. Chris Glover: Yes.

Mr. Charles Finlay: As I said, in my view, I think that maintaining the flexibility of the government in responding to the challenges that it faces is a critical principle here, so I would be concerned about the guardrails that you're suggesting—

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

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

Mr. Aris Babikian: Through you, Chair, thank you to our witnesses for coming and sharing your valuable ideas and suggestions with us. This is the first provincial-level regulating of cyber technology, AI etc., but we have to admit that as politicians, elected officials, businesses, individuals, we are always behind the curve when it comes to technology. They are way ahead of us, and we are trying to catch up with them. I believe that the most important aspect for us to properly regulate and safeguard our freedoms and our valuable information is education.

My question is to Mr. Finlay: What do you envision? How can we start planning programming and education systems so that our children—and not only the children, but also more adult people are aware of the type of infiltration, scamming, stealing your personal information? I would like to have some of your ideas because you come from an educational background, and I think that would be helpful to all of us to hear your point of view.

Mr. Charles Finlay: First of all, I think the question is extremely important about education and awareness. It is at the root of successful cyber security culture generally in our society and, I believe, at the root of effective regulation of artificial intelligence.

We need to start cyber security education at the youngest levels—very early. Some countries do this in grade school. I recommend that. We need to offer rapid education in cyber security domains that meet the workforce labour market shortage that we've talked about and that was earlier discussed that delivers workers into the cyber security sector and into these technical sectors in a matter of months, not years.

Finally, to your point about adults, we need to continue to do the work in terms of educating the public and private sectors on the work that this government has done in respect of educating the broader public sector. I think it is creditable and needs to be expanded and developed.

Mr. Aris Babikian: Thank you.

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

Mr. Brian Riddell: When I think of AI and I think of quantum, it scares me, because the speed is going to increase so much. What I'd like to ask each one of you: What safeguards do you feel we could put in to help children? I think children are our most vulnerable group and it needs to be addressed. I'll start over on the left-hand side here with you, sir.

Mr. Nye Thomas: Sure. We don't talk about the child aspects of the bill specifically, but I can talk about AI generally as it affects kids. The technology is moving really, really, really rapidly, and there's always this real potential reality of what's called law lag—you're familiar with it—particularly in technology. Technology moves fast; law is slower. How do you address that?

What we suggest in our detailed recommendations are establishing a framework for AI governance and certain obligations on all technologists, all organizations that want to use the technology, irrespective of whether it's a simple AI system or something that's more complicated. It is through that assurance of disclosure, assurance of explainability, assurance of the need to respect human rights and privacy—that's how you establish guardrails. You don't try to get into the code, if I can put it that way, of every technology, but rather you establish common expectations of those agencies, in the same way you would around their expenditure of public funds. Don't get into every expenditure, every dollar, every agency spend; rather, there are common rules every organization has to abide by. If you go outside those rules, you're accountable for it.

Mr. Brian Riddell: So the key, you would say, is be responsible.

Mr. Nye Thomas: Indeed, yes.

Mr. Brian Riddell: Mr. Finlay.

Mr. Charles Finlay: Yes, I agree with that assessment. I think that, first of all, the premise of the question is exactly right. Children and young adults are often the most vulnerable groups in terms of cyber security attacks, in terms of different kinds of technologies. Influence by state actors, in respect of younger people, we know is happening. That's a very important feature here. Government leaning in to understand data collection and understand reporting of data collection, I think, is very important. Compelling a responsible approach to how cyber security and artificial intelligence relate to children, I think, is essential.

Mr. Brian Riddell: Sir.

Mr. George Comrie: I would point out that since the very dawn of computing, there's been a problem with people—in fact, people of all ages—who kind of take at face value whatever comes out of a computer or comes up on the screen in front of them. Obviously, a certain percentage of that is misinformation and some of it is disinformation, but I think it's also very clear that the biggest vulnerabilities are around human factors, the human element of computer use more so than the technical aspects.

Having said that—and I definitely support having as much public education as possible about this—I would point out that there's still a role for the very technical pieces, which involve hardening the systems that we use for things that are critical so that we prevent them from being compromised.

Mr. Brian Riddell: So whether it's a hacker sitting in his basement in Toronto or North Korea or China or Russia, with AI and with quantum coming on the scene so quickly—

The Chair (Mr. Lorne Coe): Thank you, MPP Riddell. That concludes the time allocated for government questions this round.

We're back to the official opposition. MPP Glover, sir, when you're ready.

Mr. Chris Glover: I just want to address a question to Mr. DeVita and Mr. Comrie. In your submission, you talk about the need for training more cyber security engineers. What's the shortfall in cyber security engineers right now. How many more people do we need to train?

1040

Mr. George Comrie: Well, there's lots of statistics around it, but the last one that we reported was a 2023 statistic that came from one of your earlier presenters, ISC2. It said something like just under 40,000 for Canada and, as I mentioned earlier, it's something like a 250,000 shortfall in the United States, so an unfortunately bigger issue for them.

Mr. Chris Glover: Right, so we definitely need to get more cyber security engineers trained.

The other thing that I've heard from people when I've been talking about this bill is that public agencies, especially underfunded and small public agencies, are particularly susceptible as targets for cyber crime. You're the mayor of a small jurisdiction, Mr. Comrie. Is that the case? Do you feel like your municipality and small municipalities, small public hospitals, small school boards have the technical wherewithal or the financial resources to actually secure their data?

Mr. Brian Riddell: Point of order.

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

Mr. Brian Riddell: Again, we are not talking about funding. We are talking about the bill.

The Chair (Mr. Lorne Coe): Correct. You're outside the scope again.

Interjections.

The Chair (Mr. Lorne Coe): Just rephrase your question. We're not going to debate it. I heard the point of order.

Please go ahead.

Mr. Chris Glover: So how do we protect small hospitals, small public agencies, from cyber security attacks? Would increased funding help?

Mr. George Comrie: Yes, I was going to make the point that a lot of the public agencies simply do not have either the technical resources or financial resources or human resources to deal with what they're being asked to do in Bill 194. I see that that is a potential problem; they need technical assistance, but ultimately, for some of them, it's going to be a financial issue.

Mr. Chris Glover: Right, thank you. I'll pass it to MPP Wong-Tam.

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

MPP Kristyn Wong-Tam: Thank you, everyone, for your presentations today. I'm interested in understanding the difference that we've heard so far from deputants who've come forward between yesterday and today. There are those who are specifically saying—for example, yourself, Mr. Finlay—to proceed without the regulations at warp speed. Then we have others who are asking for more information, asking for specific guideline principles to be set up front, which will then guide the rest of the delivery of the bill, including the regulations.

I'm just trying to understand. We've got two different opinions coming back and forth, and there's been no consensus whatsoever that this should just go ahead as is—that, I think we can agree on, because everybody's asked for some changes to strengthen the bill.

I'm going to start with the Law Commission. You're asking us to be cautious and prudent and to use best practices, including building on what's already available. Others are saying, "Go ahead." Can you speak to that difference?

Mr. Nye Thomas: Sure. The context we're operating in is that we are interested in protecting rights—human rights, privacy, procedural justice rights—because AI systems used by government agencies and governments make decisions affecting those rights, so there are certainly fundamental transcendent legal obligations they have to abide by. We don't think you should be too risky when it comes to rights protection.

We don't think you should be too far out there when it comes to ensuring that privacy rights are protected, for example, or human rights are protected. Therefore, we believe the bill would be improved if it adopted more of the commonsense consensual principles of AI that are being adopted around the world, based upon their experience. Our comparative or competitive jurisdictions—the United States, Europe—don't want to frustrate AI; they want to promote it the same way we do, but they have learned through experience that you need a more sophisticated safety net than I think is present in the bill right now, absent amendments.

MPP Kristyn Wong-Tam: I have two and a half minutes left. Charles, if you can provide us with a quick answer?

Mr. Charles Finlay: In my view, the protection of rights that already exists in the charter, in the Ontario human rights act and other statutes is a sufficient guardrail in respect of the regulations that could be passed, and I urge speed, flexibility and agility in these regulations to meet this kind of innovative pace.

MPP Kristyn Wong-Tam: Thank you. I'm just going to pick up before the engineers pop in, because this is actually the other point of tension, I think: We have heard from the Information and Privacy Commissioner, who was really clear in her remarks that we needed to have a human rights approach embedded in the framework of the legislation, which currently does not exist today. We also heard from the minister, who wasn't able to land on a commitment, even though he was asked a question two or three times by my colleague, on embedding that human rights approach.

May I just open this question to you one more time? I'll start with the law commission. The human rights approach that the accountability officer, the commissioner, has asked for is not embedded in here. There has been some assertion that the charter should be enough, that the Human Rights Code should be enough, that you don't need the language in here. How would you respond to that?

Ms. Susie Lindsay: Thank you for that question. It's a great question. The work that we do in law reform is really to see where the gaps are and to make recommendations to improve or fill those gaps.

This is a gap, and yesterday the commissioner of the Human Rights Commission was correct, obviously, that the government has an obligation to provide services that don't discriminate. The concern is, in the jurisdictions that have very similar human rights frameworks—we're talking Pittsburgh, Wisconsin, Australia, Denmark, the Netherlands—they've shown harms in government deploying AI systems that have been discriminatory, so we know that human rights frameworks that align with ours are not sufficient.

Number two, our human rights framework is an ex post assessment, so after things have gone wrong, someone makes a charter claim. Someone brings in the Human Rights Commission, and we look at it in hindsight. The—

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

We're now going to move to the government members for their second round of questions. MPP Sarrazin, please, when you're ready, sir.

Mr. Stéphane Sarrazin: Thank you, all of you, for the presentation; it's quite interesting. I had the chance to sit on the parliamentary assembly of francophones which gave me the opportunity to meet with many parliamentarians from European countries. We had—probably like you—many symposiums, workshops, meetings and consultations on AI, and what I think I've noticed is that everybody wants to wait until they have the right legislation. I think it's important now to go ahead with a legislation and be able to adapt it afterwards with regulations, and I would like to ask all three organizations: Do you agree with that?

Mr. Nye Thomas: In principle, I agree with you. With law reform, you learn from experience. You start somewhere, get some experience under your belt and you adapt. The problem with this legislation, if I may say, is that it just isn't quite at the starting line yet, if I can be so bold.

The EU AI Act is 140 pages long. The executive orders that govern AI in the federal government in the United States are 60 pages, plus hundreds, if not thousands, of pages backing that up. In contrast, in Bill 194, the AI sections are about a page and a half long. I don't support 150-page legislation, no way. I think that's overreach, overregulation; you're asking for trouble.

But I think what we've got now is a little too skimpy, and we can agree that law reform has to be iterative, but I think we need to move the starting line a little further down the road. That's our recommendation.

Ms. Susie Lindsay: Can I just add to that that we would support accepting all of our amendments? Then we would support the bill.

Mr. Stéphane Sarrazin: But you agree that we need to move on this.

Mr. Nye Thomas: Yes.

Mr. Stéphane Sarrazin: That, I think, is the most important part.

Mr. Peter DeVita: We've entered an era where technology is forcing our democratic processes to change. We can't respond fast enough, so legislation has to become much more nimble—which you are talking about; that's a correct step—but it also needs to be well-informed. You can't afford to make mistakes in these nimble decisions, so you need to have mechanisms that advise the minister—an advisory council—and I would also recommend that we put in the act the ability for the minister to specify the qualifications of the people who actually practise cyber system security and get into AI systems. You need to get down to who is actually doing this and who is being responsible for all the things that you're talking about. Somebody is actually doing this kind of work. So that needs to be paid attention to. Thank you.

1050

Mr. Stéphane Sarrazin: Would you like to comment?

Mr. Charles Finlay: Yes. I agree with both other panellists in respect of the urgency of this issue. We need to move on this legislation right now. There is absolutely no time to waste. I certainly understand the need to get it right, and I certainly understand the need to observe and protect human rights. That's obviously critical. But I would observe that human rights are being violated by the cyber attackers. They're being violated by nation-states that, quite frankly, are averse to what we're doing in this room. So I respectfully encourage this government to move forward with this legislation without delay.

Mr. Stéphane Sarrazin: Thanks.

The Chair (Mr. Lorne Coe): I have MPP Babikian, please, to begin, followed by MPP Saunderson.

Mr. Aris Babikian: Like any other industry, like any other new technology, there is always the first to catch up with, to start regulating. Every country around the world, they have a different constitution, different operational, political system, etc. Each one of those countries will adapt to these challenges according to their own culture, traditions, constitutions.

Here in Ontario, we are trying to regulate something that is such a wide field that no one can imagine that we will have an answer to everything. I mean, all of you, you have very valued and valuable input, but to sit down and start negotiating or debating—you mentioned a 140-page bill. It's not practical. I think once we set up the legislative framework, the regulation is the best place for us to include all your suggestions, input and also catch up with the new development coming down the road which we cannot foresee.

So don't you agree that the regulations—we should leave all these questions and challenges and suggestions to the regulations to address many of these things?

Mr. Nye Thomas: If I may answer for the law commission: We don't agree everything should be left to regulations, as I say. We know what the comparators are; we're not recommending 140 pages of amendments. If you look at—again, that would be crazy. We do not support that. What we support and what we recommend are comparatively brief, common-sense regulations based upon experience so far.

You say we don't know all the risks. That's certainly true. We know some of the risks, though. We know some of the outside risks, because we have experience with them in other jurisdictions; policing is one, use of certain AI systems around child protection is another. So we aren't starting from zero. If we want to start with a good floor—that's really what we're talking about. If we want to start with the best floor we can conceive, we should be mindful of adding to the current legislative framework some of the common-sense, I think, fairly modest and conservative recommendations that we're recommending in our submission.

The Chair (Mr. Lorne Coe): You have 50 seconds remaining, so you might want to make sure your responses are precise.

Mr. George Comrie: Okay. I would say that I support the principles being in the legislation, the higher-level principles. The next level of detail belongs in regs, it seems to me, and then there's a level of detail that happens outside the regs, which is what my colleague was referring to earlier. You're relying on competent, professional people to follow the principles that are there.

You know, the Brits have a concept called "right-size regulation," maybe you've heard about this. That's the difference between the 140 pages that the EU has, that they're going to collapse under, and something that makes sense and is manageable. Trying to strike that balance is the trick behind this, frankly.

The Chair (Mr. Lorne Coe): All right. We're concluded for the government questions. This concludes your presentations to us this morning. Thank you for being with us. We wish you well. Have a good weekend.

ASSOCIATION OF MUNICIPAL MANAGERS, CLERKS AND TREASURERS OF ONTARIO

IBM CANADA

The Chair (Mr. Lorne Coe): I'd like to call forward, please, the Association of Municipal Managers, Clerks and Treasurers of Ontario, and IBM Canada. Please come forward and take your seats at the table.

We will start with the Association of Municipal Managers, Clerks and Treasurers of Ontario. For the record, sir, please identify yourself. Then, you will have seven minutes for your presentation. Start, please.

Mr. David Arbuckle: Good morning, Chair Coe and committee members. My name is David Arbuckle. I'm the executive director for the Association of Municipal Managers, Clerks and Treasurers of Ontario, or AMCTO—little easier for you. We're Ontario's largest voluntary association for municipal professionals in the province. We have over 2,200 members in almost every municipality in the province, including CAOs, clerks, treasurers, bylaw enforcement officers, solicitors, as well as other municipal professions. Along with training, education and leadership, we research and develop policy ideas that improve the ways municipalities function and provide services to the public. Thank you for the invitation today to attend.

I'm here to highlight a few items that are really important to our members: the interconnectedness of cyber security, AI and municipal privacy protection throughout legislation; the vast differences in municipal digital maturity, capacity and resources; as well as policy, guidance and tools that municipalities require. With Bill 194, as digital services expand and citizen expectations evolve, AMCTO advocacy has been focused on giving municipal administrators the right legislative tools and guidance to manage the impacts of technology on service delivery. Privacy, security, data and system vulnerability, algorithmic bias and lack of transparency have all been identified by our members as key issues. Our members want to ensure fairness, transparency and protection of privacy with the use of AI technologies.

As an association, we see Bill 194 as a very good first step in this direction and AMCTO supports its overarching goals to enhance digital security and establish trust across public sector institutions. As an association, we recognize that Bill 194 is enabling legislation that will help guide future regulation development as well as future legislation. We can appreciate the need for legislation to remain flexible and relevant in the face of technological and societal change and understand that implications for municipalities will come at a later phase.

That being said, more legislative clarity around roles and responsibilities and appropriate use of AI would help municipalities understand their obligations and their requirements. In addition, other stakeholders have flagged inconsistency challenges when legislation and regulations are phased in across sectors, creating different levels of privacy protection within the public services. Even if phased in, potential spillover effects of legislation and on-the-ground implementation impacts for the municipal sector should be considered when moving forward.

With the technological challenges facing the sector, it is more important than ever that the province help municipalities embrace the digital world with responsible mechanisms in place while providing flexibility to adapt to local circumstances, and in a way that respects the spectrum of digital maturity.

1100

I want to just talk briefly about MFIPPA. The design and use of AI systems make it difficult to control information as it flows to and from AI systems or the cloud. Tech companies have rolled out AI without easy opt-out, really tasking the clerk, who is often the head of the institution under the Municipal Freedom of Information and Protection of Privacy Act, with ensuring their organization is ready for AI.

Looking broadly at local services, clerks are also responsible for running local elections. We hear increasing concerns about the rapid spread of misinformation, deepfakes and other materials created and spread through technology like AI, and the potential impacts on voters. We need to look at a broad range of service impacts with regulation.

Subject to collaborative consultation and having supportive resources in place, AMCTO supports extending similar proposed provisions of FIPPA to MFIPPA. However, in its current state, MFIPPA is onerous, lacks clarity, creates additional unnecessary work and is not equipped to consider important technology trends. Local government administrators need a modern MFIPPA before adding new provisions to an old act. It has been over 30 years since MFIPPA has been comprehensively reviewed; the legislation still references CD-ROMs as an appropriate manner to communicate information.

It would be most effective if rather than through amendments, provisions needed to come with a comprehensive overhaul of MFIPPA, as well as a privacy lens placed on other legislation including the Municipal Elections Act. AMCTO recently has done a full comprehensive submission on the need for an update of MFIPPA. We're glad to say that we've had very encouraging conversations with Minister McCarthy and his staff about future direction as it relates to MFIPPA.

We would encourage the committee and the government to account for operational nuances and differences in municipal structures, size, finance, financial and human resources, and digital maturity. Legislative, regulatory, monitoring, enforcement and reporting proposals should be co-developed with municipal leaders and stakeholders, along with IT, procurement and risk-management professionals.

Municipalities are at different stages in their digital journeys. Some are advanced in the use of privacy impact assessments; others are not. Some are ahead of the plan when it comes to AI implementation; others don't even know where to start. Smaller municipalities often lack technical expertise, with fewer staff resources, choosing to contract out IT and shared services.

Consideration should be given to a minimum or a scale of standards. If there's one set of compulsory standards and metrics, smaller municipalities may be challenged in implementation. When it comes to reporting requirements, consider opportunities to minimize the burden. Over 60% of municipalities are under 10,000 people, so again, a blanket approach may not meet the needs of the majority of municipalities.

In closing, we'll talk about how frameworks, policies, protocols, road maps, best practices, governance structures, guides and training programs are needed to help navigate the challenges and leverage opportunities. Regulations must be flexible, built-in to respond to local circumstances and paired with funding for implementation.

The province has asked and continues to ask a lot of municipalities with limited available funding for implementation. Our members are asking for comprehensive legislative change, flexibility for local circumstances, and appropriate guidelines and resources to improve on service delivery, privacy protection and security. Thank you, sir.

The Chair (Mr. Lorne Coe): You're right on time. Thank you very much, sir.

Mr. David Arbuckle: I did my best.

The Chair (Mr. Lorne Coe): I'll now move to IBM Canada. Sir, before you start, I need your full name and title with IBM Canada.

Mr. Tiéoulé Traoré: Tiéoulé Traoré. I'm the government and regulatory affairs executive for IBM in Canada.

The Chair (Mr. Lorne Coe): Welcome to the committee, sir. You have seven minutes. You can start.

Mr. Tiéoulé Traoré: Thanks for having me. IBM Canada is thankful to be here today to offer its views on legislation we believe will set Ontario up for success when it comes to implementing an AI framework that can uphold the rights of Ontarians, while stimulating innovation.

This opportunity is very apropos for us; we're celebrating this week the fifth anniversary of our ethics board, an internal function that has been instrumental in ensuring that IBM's world-class IT technology in consulting services, including AI, are rooted in ethical principles from inception to delivery.

IBM is a multinational company, and as such, has operations all across the world, including here in Canada, a country we have nurtured deep roots in for now close to 110 years. Here, it starts with Markham, our home. This is where we're headquartered, and this is where, through our software lab, the largest-such facility in all of Canada, we develop from start to finish made-in-Ontario AI solutions for the benefit of all.

IBM has long championed AI to do good. Yes, this technology serves as a formidable driver of growth. It led globally to a 25% increase in revenue, according to this year's edition of our AI in Action report. At their very core, the best AI case studies are the ones that improve customer experience.

That is why IBM endorses Bill 194 and sees it as a positive first step. The global pandemic highlighted how technology leveraged to do good could help governments from across the world reach out to their respective constituents and deliver crucial services in a prompt and reliable fashion. AI is indeed a core component of digital governance strategies and can aptly meet the growing needs of citizens when it comes to ensuring service delivery is the same regardless of your area of residence. AI bridges linguistic and geographic divides, a must in a country as large as ours.

This bill sets what we see as winning conditions for the dual growth of the provincial economy and the consistent well-being of Ontario residents by targeting two sectors with vulnerable segments of populations: health care and education. It does so with three foundations that are unavoidable to earn and uphold the public's trust. Yes, AI can be disruptive, and models improve at a frenetic pace, and without the right governance model, we stand the risk of losing the people's buy-in. Bill 194 smartly avoids these concerns by promoting a framework centred on governance, cyber security, and privacy.

My objective today is to highlight what IBM sees as important provisions to ensure that Bill 194 meets its lofty goals, considerations we believe will bring added value to the already-strong proposed framework.

On the AI front, Ontario should strive to promote innovation, public safety, international harmonization and clear responsibilities along the AI supply chain. As such, it should:

—encourage an open-source framework where proponents collaborate on community-built technology and the open exchange of ideas, skills and culture to promote safety, foster competition and protect security interests;

—adopt a risk-based approach, with regulators focusing on high-risk situations resulting in serious harms to Ontarians, with the objective to regulate risk, not algorithm;

—adopt the OECD's definition of AI as a "machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate output such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment"; and finally

—articulate clear responsibilities across the AI supply chain. Developers, or producers, produce the AI model and system, while deployers, or providers, determine the use case of the model. As such, deployers are best positioned to document and assess risk associated with specific use cases.

On the cyber front, Ontario should avoid the victimization of victims via overly punitive compounding fines. Breaches are more often than not the result of sophisticated bad actors, not gross negligence. Allow for a reasonable reporting window in the event of a breach—72 hours is a standard levied in mature cyber jurisdictions—and allow injured parties to best-understand what went wrong, which will in turn feed regulators with more insightful feedback. Offer liability protection for private sector sharing of information; actors with reasonable risk management systems and programs should be shown leniency.

Finally, in the field of privacy, Ontario must place primary accountability for the protection of personal data on controllers or providers; promote privacy-enhancing solutions like anonymization and pseudonymization of personal data; and, finally, provide data subjects with basic rights with respect to their data—what is being collected, why it is being collected, how it would be used and where to access it—while balancing fundamental rights and freedoms.

We believe these recommendations will help the Ontario government maximize the reach and efficiency of a framework already carrying the right foundations. We hope ensuing regulations do incorporate these essential provisions.

Thank you very much for listening. I will be happy to address your questions.

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

We're now going to start with questions from the official opposition, and I have MPP Glover. Please, sir, when you're ready.

1110

Mr. Chris Glover: Thank you both for being here today and for your presentations. I'm going to start with a question for Mr. Arbuckle. I heard a number of things that I'm quite interested in pursuing from your presentation today. You said you support the overarching goals of the legislation and you understand that it's enabling legislation, but you said that it needs more definition of roles and responsibilities, as well as the appropriate use of AI.

The Information and Privacy Commissioner has recommended a certain statement be inserted into the legislation, and that statement—let me just read it here—is that AI should be used in a manner that is valid and reliable, safe, protects privacy and is transparent, accountable and human-rights-affirming. Would you support that insertion into this legislation?

Mr. David Arbuckle: Thank you for the question. Through you, Chair: I think overall we would support having more information than less. So, ultimately, if certain principles are written within the legislation that will allow members to feed back and respond to it, then we would encourage that. Certainly, that aligns with our need for greater clarity in relation to some of the legislative changes.

Mr. Chris Glover: What I've heard from a number of small public sector agencies is that they have trouble protecting the data that they are in charge of because they just don't have the financial wherewithal, or they don't have the technical expertise. Is that your understanding as well, from the municipalities that you represent?

Mr. David Arbuckle: Through the Chair: Yes, certainly we would echo that. From a municipal perspective, as I mentioned in my comments, a lot of them are smaller municipalities, less than 10,000 people, sometimes having as few as five staff. So ultimately, those responsibilities in relation to privacy and technology fall on the corner of someone's desk in a small municipality, and ultimately they may not have the tax base or the wherewithal or the expertise in order to implement that.

Our members are very creative, and our members look to their neighbours, look to other jurisdictions, to see where there's opportunity to make improvements, but there certainly are challenges from an implementation perspective and financial perspective.

Mr. Chris Glover: So in the implementation of this bill and the requirements—the cyber security requirements, the AI requirements that the government is going to be imposing on municipalities—would it be helpful for smaller municipalities in particular to have specific programs available centrally from the provincial government and financial support to implement those programs to protect the data that they hold?

Mr. Brian Riddell: Point of order.

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

Mr. Brian Riddell: Point of order: Again, this is discussing funding, which is not in the scope of this bill.

The Chair (Mr. Lorne Coe): Understood.

Can you please bring it back to the scope of the bill?

Mr. Chris Glover: Okay, yes. Let's see. Should the province provide programs and financing for municipalities to fulfill the requirements that are going to be imposed on them?

Mr. David Arbuckle: Thank you for the question. Through the Chair: We would ultimately look for the province to provide greater resources as it relates to the implementation.

Now again, in our discussions with the ministry, municipalities aren't the specific target in relation to this particular piece of legislation, although we've highlighted the fact that there is the potential for spillover opportunities within the regulation. So ultimately it would be our position that the province support municipalities of all sizes as it relates to the implementation through a number of mechanisms, which I mentioned in my comments around guides, and funding could be one of those resources as well.

Mr. Chris Glover: Thank you so much.

And then my next question will be for Mr. Traoré. You talked about the minimization of data while balancing fundamental rights and freedoms. Would you be supportive of inserting into the legislation the statement recommended by the Information and Privacy Commissioner that AI should be used in a manner that is valid and reliable, safe, protects privacy and is transparent, accountable and human rights-affirming?

Mr. Tiéoulé Traoré: I'd have to see what this initiative is with regard to international partners, because we're not operating in a vacuum. I think with something as serious as AI, we would want to make sure that the move that we're making, be it as a province or a country, is aligned with that of more mature jurisdictions. But this is certainly something that we would look at.

Mr. Chris Glover: Okay, thank you. So you just need more time to consider that? It is from the EU AI Act, actually, but we could have a further discussion afterwards.

I'll go back to Mr. Arbuckle. You talked about surveillance by—you mentioned surveillance and the risk—sorry, I'm actually on the wrong note here. My apologies.

Let me just ask a broad question. What do municipalities need in order to protect the data that they're already in charge of? Because right now, we've had a number of municipalities and public sector agencies that have been hacked, and it's cost them millions and millions of dollars. The average hack costs $6.3 million. What do municipalities need right away in order to protect their data?

Mr. David Arbuckle: That's a pretty broad question, but ultimately it comes down to IT infrastructure—so do they have the appropriate IT infrastructure and the tools in place? There also needs to be a discussion in relation to available resources for those municipalities to bring in experts to be able to provide them with the expertise. Because again, as we mentioned before, there are a number of smaller municipalities that don't have that internal expertise and won't have that internal expertise. So ultimately, they have to be able to access those things and those things ultimately cost money.

Mr. Chris Glover: Thank you.

How much time is there left, Mr. Chair?

The Chair (Mr. Lorne Coe): You have a minute and six seconds.

Mr. Chris Glover: I'll pass it to MPP Wong-Tam.

MPP Kristyn Wong-Tam: A minute and six seconds? Okay, sure, thank you.

Many of the school boards, hospitals, post-secondary institutions are currently running deficits. They're selling off assets, they're scraping by with lines of credit. I'm just curious to know—and this includes municipalities as well—what would be the consequence of not being able to deliver upon the government's new request of you, if they're not resourcing you for success?

The Chair (Mr. Lorne Coe): In 31 seconds.

Mr. David Arbuckle: Thank you. Through the Chair, ultimately municipalities would have to look at opportunities to be creative to meet the legislative requirements, but it certainly isn't unusual for governments—not the government, but governments in general—to provide regulations and not necessarily provide the resources in order for municipalities to implement. Ultimately there would have to be a discussion between the government and the municipal sector in relation on how to properly finance those obligations.

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

I have MPP Saunderson. Sir, when you're ready, please.

Mr. Brian Saunderson: Thank you to both presenters for coming in today and sharing your expertise with us on this important initiative. You guys are our last panel, so we saved the best for last—congratulations.

We've had two days of hearings now. We've certainly heard that this is an urgent situation and that with topics like AI, we're playing catch-up right now, and so I wanted to drill down. Would you agree with that, that we're playing catch-up right now, that this is a situation that has to be addressed immediately?

I'll start with you, Mr. Traoré.

Mr. Tiéoulé Traoré: This is a technology that is evolving at a frenetic pace, so we certainly understand the need for governments across the globe to ensure that they have the right regulatory framework to secure the buy-in that's absolutely needed, because AI feeds on data. That data belongs to the people, so of course setting up the right narrative and the right framework to make sure that said data is used in a way that is responsible is key. At the same time, the disruptive nature of AI can really do a lot of good in the context of tackling current issues and future ones.

So, yes, the time is definitely now.

Mr. Brian Saunderson: Mr. Arbuckle?

Mr. David Arbuckle: Through the Chair, certainly there are a number of municipalities that are on the forefront in relation to using AI for things like service delivery, customer response, infrastructure challenges, but they are doing so in the absence of legislation and a framework of legislation and guidance from the provincial government.

So yes, certainly, ultimately, as we mentioned before, we think this legislation is a really good first start to help provide the broader public sector, including municipalities, with that guidance.

Mr. Brian Saunderson: Going into the municipal sector—because I have some experience there, and it's an important one. It's really our first line of politicians for our residents at our most granular level.

You've talked a bit about the divide; there's the large municipalities and the smaller municipalities. You mentioned there's many municipalities across Ontario—I think it was almost 60% that have less than 10,000 people?

Mr. David Arbuckle: Correct.

1120

Mr. Brian Saunderson: That's over 260 municipalities, roughly, then.

I want to get a sense, then, on the relativity. We've certainly heard about cyber attacks; they've hit large municipalities like Hamilton and smaller municipalities. It was quite devastating in Stratford. There was one municipality in my riding of Simcoe–Grey that was hacked, and that had devastating consequences and brought the town to a halt, really.

Based on the size of the municipality, cyber security is a huge issue. And then AI is probably an issue, but only for the larger municipalities, I would think, that have the bandwidth to make those investments. Can you kind of break that out for me?

Mr. David Arbuckle: Yes. Thank you, and through the Chair, certainly, I think we're looking at—again, you're right: There is a different discussion that occurs in relation to cyber security versus AI, but there are a number of smaller municipalities that, again, are on the forefront in relation to using AI. King township is one that I could use an example, who has been very forward in relation to using AI as far as a customer service tool and modernizing their customer service.

But ultimately, again, we're looking for legislation and regulations that ultimately recognize the differences in relation to that capacity. As I mentioned in my remarks, we're looking for more minimum standards in relation to the regulations so that municipalities of all sizes can ultimately meet and exceed that legislation, because a lot of municipalities aren't necessarily satisfied with meeting the regulations. They want to do the best in their own local interests. The minimum standards will allow municipalities to be able to meet the needs of the legislation and regulation but also respond to the needs within their own communities and their own capacity.

Mr. Brian Saunderson: Just to drill in: Again, if you were breaking it down between cyber security needs and AI needs—because we've been talking about bandwidth and resources, and we've heard from previous presenters that there's a shortage in AI-trained individuals and cyber security as well. If you were grading the demand in percentage, what would be the relative breakdown for cyber security versus AI for most municipalities, for most of your members?

Mr. David Arbuckle: Thank you for the question. I don't think I can answer that question, MPP Saunderson. I don't have that breakdown for you.

Mr. Brian Saunderson: Okay. Continuing, then, you talked in your comments about scalable standards, because you're trying to get certainty in an area that's very in flux and changing dramatically. Probably in the time we've been talking over the last few days, there's been more changes in the AI world than we could have imagined. Can you describe for me or explain to me what you're looking for or referring to when you're talking about scalability in the standards? I'm assuming it would relate to the size of the municipality and that it would be kind of fluid. Can you take me through what that would look like?

Mr. David Arbuckle: Through the Chair, I don't think from a technical perspective I could, but again, we've seen legislation in the past that ultimately treats municipalities as one entity. You look at things like the AODA Act, as an example, where there were certain requirements in relation to accessibility put on municipalities. Again, some larger municipalities may have more ability through internal expertise; through their access to resources, to consultants, to technology; through procurement. They may have more access and more sophistication as it relates to their access there, whereas some smaller municipalities may not have that opportunity, or it may take them longer in order to make that implementation.

Ultimately, that's what we're looking for: that there's not just one-size-fits-all regulations that are put forward, but there is some recognition and some flexibility within those regulations that allows municipalities to meet that standard but do so at a pace that's appropriate for their communities and their residents.

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

Mr. Brian Riddell: To Mr. Arbuckle: To support the broader public sector and municipalities, the Ontario government provides cyber security standards posted on ontario.ca, advisory services, best practices, guidance and educational awareness to help strengthen and build cyber security resilience across the province.

The Ontario government has also made resources available through the Cyber Security Centre of Excellence and the Cyber Security Ontario Learning Portal to BPS organizations and municipalities so they can better equip, protect and educate organizations and can receive assistance in the event that they are victims of a cyber security attack.

The Ontario public service's Cyber Security Operations Centre operates 24 hours a day, seven days a week, 365 days a year to—

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

We're now back to the official opposition for your final round of questions, please. MPP Wong-Tam.

MPP Kristyn Wong-Tam: Just coming back to the importance of municipalities and all those who work within the sector needing to be trained, but also this type of training requires specialized skills—I recognize that municipalities may not have that on staff, rendering them having to contract out, bring in outside consultants. Obviously, municipalities may not be developing their own proprietary software. Oftentimes, they have to purchase through licensing agreements.

I'm just curious to know the protocols that exist today when municipalities, large and small, have to buy software; whether or not they're purchasing that software for procurement, if it falls under the fairness monitor; and how do they do it if they're not resourced, necessarily, for all of that success.

Mr. David Arbuckle: Through the Chair: Ultimately, all municipalities are required to have some sort of procurement bylaw. Those procurement bylaws are based on best practices within the sector. If they are doing some sort of assessment within the municipality to be able to identify the gaps from a cyber security perspective, they would look through their procurement bylaw to see how they can resource that tool.

There are a number of organizations—LAS, through AMO, provides a service in relation to some of those procurement tools that they may be able to access. So there is some support to municipalities.

Just to recognize MPP Riddell's comments: Municipalities do routinely look to that cyber security centre as well, and our members have also provided a lot of resources to that centre, giving them some ground-level expertise in relation to what's happening on the ground. We've taken the opportunity to share a lot of those resources from that centre with our members.

MPP Kristyn Wong-Tam: That cyber security centre operated by the province doesn't replicate, nor does it stand in place of, municipalities on their own delivering that service. It's sort of like a website, a guide, someone on the phone, but you still need someone on the municipal side that actually implements the work.

Mr. David Arbuckle: Correct.

MPP Kristyn Wong-Tam: To MPP Glover's point about having the appropriate resources, are municipalities today ready for this? Municipalities and all your municipal agencies, because libraries, recreation centres, public health units are attachments to you: Are you folks ready and resourced to actually take on this legislation?

Mr. David Arbuckle: Through the Chair: Ultimately, that's part of the challenge, right? As I mentioned in my comments, there are varying degrees of sophistication and capabilities within those municipalities.

Sometimes, it's not really dependent on size. There are large municipalities that aren't as sophisticated as other large municipalities. There are varying degrees in relation to that capacity and their readiness to, you know, adopt things like AI, and adopt different skills and different technologies as it comes forward.

That's part of our message today: Yes, there are some that are ready and prepared, but the world continues to change and that readiness continues to change as well. So having the resources in place and the expertise in place in order to respond to those changes is important for the sector.

MPP Kristyn Wong-Tam: How many municipalities do you represent?

Mr. David Arbuckle: We're a member-based organization. We represent individuals, so 2,200 members. But we actually have members in almost all 444 municipalities.

MPP Kristyn Wong-Tam: Right. And out of those 400 municipalities, would you be able to share with us a sense of how many municipalities are capable, ready and resourced, to respond to this legislation adequately?

Mr. David Arbuckle: We could probably go back and look to see what sort of plans they have in place in order—cyber security plans, all of those other sorts of necessary plans in readiness for adoption. We could go back and check that. I don't have that data with me, though.

MPP Kristyn Wong-Tam: Thank you. I spent 12 years at Toronto city council and I remember the auditor general coming forward to share with us a very bleak report about how exposed the city of Toronto was to cyber security attacks. She was able to randomly go to a number of municipal outlets—recreation centres, libraries, civic centres—open up her laptop, and even though she would admit that she's a Luddite, she was sophisticated enough to be able to hack our system, to penetrate the system. The city of Toronto has a $14-billion operating budget and almost a $30-billion capital budget, and yet we were not prepared for what she had to share with us. I know that we have a department now at the city that really is tasked—it's a full-time department with dozens of people employed, working around the clock to make sure that our systems are secure; our data, on behalf of the citizens, while collected, is secure. It is a constant battle because of the evolving and emerging threats.

1130

I think about the 60% of the municipalities in Ontario that have populations less than 10,000 people, that probably are not as well resourced as Toronto, and I worry that those municipalities will be left behind. Those smaller municipalities could become the big aggregate target of those who want to do harm to our citizens, including foreign states.

So I'm curious to know—because you've cited that we should not have a one-size approach, which I think is very astute: What would it look like in order for us to protect those smaller municipalities? What do they need?

Mr. David Arbuckle: Again, through the Chair: Our approach and recommendation is that when regulations are being developed, ultimately, those regulations are scalable. So, ultimately, is there a minimum standard that can be provided that will provide smaller municipalities as well as larger municipalities with guidance so that when they are moving forward in relation to adopting AI technologies or adopting different technologies—that they have those minimum standards in place that will ultimately assist them in that delivery?

MPP Kristyn Wong-Tam: Thank you.

Mr. Traoré, my final question is to you. This piece of legislation applies only to public institutions. The government is not making this legislation apply to private actors like IBM or Dell. Do you think the industry would benefit from having legislation that also regulates how you manage and control your data?

Mr. Tiéoulé Traoré: We're certainly open to it. Looking at what the federal government is trying to do through C-27, the idea was not—

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

MPP Riddell.

Mr. Brian Riddell: To Mr. Arbuckle: You realize that the Ontario public service's Cyber Security Operations Centre has a Supply Ontario vendor-of-record list for accessing cyber products and services, and that we support a secure governance framework for including technical and operational cyber security policies and standards. Would you acknowledge that?

Mr. David Arbuckle: Yes, sir.

Mr. Brian Riddell: Over to IBM: I always remember Big Blue—that's a long time ago now. You look from there to today, and you look at AI, and you look at quantum computers—it's never-ending. But do you support this legislation?

Mr. Tiéoulé Traoré: Yes. I think this legislation is a strong first step. The use case is really going to define, ultimately, the success of this legislation, but there is a lot to like, through the foundations that are being leveraged.

Strong governance is going to be key, obviously. We want to make sure that the trust that is bestowed by the public is upheld, and that Ontarians are confident that the use cases are going to respect their data and are truly going to do good.

Cyber security is key. The cost of a cyber incident in Canada, on average, is $6.28 million, which is colossal. That's a figure which incorporates businesses of all sizes, and government and academia. This is a figure that skyrockets to $9.32 million for breaches to critical infrastructure like financial institutions or IT systems. Cyber security is paramount. We need to make sure that there's resiliency when it comes to our infrastructure, and then again, it all harkens back to privacy. That data is key, but that data needs to be protected at all costs.

And we need to know who does what. AI is a supply chain. This is something that's very important to remember. We all play a part. We all have responsibilities. We all have obligations; they're just not the same. So we need to make sure that we all know what to do along the supply chain and we uphold our commitments.

Mr. Brian Riddell: Based on that and the fact that to protect children and institutions we need to move quickly, the minister should have the authority to be nimble and make decisions as required.

Mr. Tiéoulé Traoré: Through the use case and the added value of the targeted subjects that are going to benefit from this legislation, we believe that it's important to act, but more so act strongly, and to make sure that through the regs, as you try to operate this legislation, all the safeguards that are embedded in principles in this legislation, in this text, see the light of day.

Mr. Brian Riddell: Now I'll pose those questions to Mr. Arbuckle. If you want me to repeat them, I will.

Mr. David Arbuckle: You may need to repeat the first one, but I'll respond to the second one. The idea in relation to moving swiftly through the regulations: We certainly appreciate, given the issue at hand, that there may be a need to move more expeditiously with the regulations. However, we would highlight that in that reg development, we would expect some sort of consultation and some sort of conversation that happens with affected stakeholders within the public sector so that, ultimately, their expertise and their experience can be brought to bear in relation to the regulations.

Mr. Brian Riddell: Thank you for your answers. And I'll—

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

Through the Chair, we have MPP Sarrazin. À vous, s'il vous plaît.

Mr. Stéphane Sarrazin: Through you, Chair, I would like to thank you both for presentations and, Mr. Arbuckle, for your advocacy towards municipalities. Prior to being an MPP myself, I was a mayor of the small township of Alfred and Plantagenet in Prescott-Russell. Et j'aimerais aussi remercier M. Traoré de nous avoir partagé vos expertises, puis aussi, je pense que vous travaillez aussi avec des organisations francophones en Ontario, donc merci. C'est vraiment intéressant.

Going back to the municipality, we've talked earlier about what was available for municipalities. I remember as a mayor in 2018, with my small municipality of 10,000 in population, getting almost $1.5 million from this government through the modernization grant, or whatever, something that was offered to increase efficiency to municipalities. You know, $1.5 million for a population of 10,000—I think that was great, and we did manage to do great things, like a cloud system to be able to better answer the needs of our—and I'm glad that you're here to talk about this. I know when I was actually sitting as a mayor, we were more worried about being sued if there was some data compromised and investing in the actual resource to prevent this from happening. One thing that we came up with, which was great at the time, is that the upper-tier municipality would take care of all these small municipalities when it comes to IT needs, and it was a big difference. You've probably heard some of our small municipalities were victims of ransomware.

Thinking about all this, how can any future potential regulation take municipal needs and interests into account when providing governance and guidance to municipalities?

Mr. David Arbuckle: How much time, Chair, do I have?

The Chair (Mr. Lorne Coe): You have a minute and three seconds.

Mr. David Arbuckle: I will be very efficient with—

The Chair (Mr. Lorne Coe): Your colleague from IBM might want to jump in.

Mr. David Arbuckle: Yes. Just one item I want to cover is insurance costs. Again, even in the last year, we've seen upwards of a 7.5% increase to cyber insurance costs at the municipal level. Previous to that, we had seen over a 20% increase, and that, as you know, in a small municipality, can hit you pretty hard.

Our members have really reiterated that there needs to be a balance within regulations to minimize risk and protect privacy, while at the same time avoiding stifling innovation. That's the last thing I think municipalities want to do.

So again, we want the standards for AI to guide safe, responsible, ethical use and specifics around AI-driven cyber threats. Those would be some of our high-level concerns as it relates to the development of those regulations.

Mr. Stéphane Sarrazin: If I can add, Mr. Chair—

The Chair (Mr. Lorne Coe): You've got 10 seconds, sir.

Mr. Stéphane Sarrazin: So you both agree that we need to go ahead with this regulation, with this legislation? Because we can't talk about it forever and not make it happen—

The Chair (Mr. Lorne Coe): That concludes the time for questions. That concludes our public hearings on Bill 194.

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 9 a.m. on Thursday, November 21, 2024. Thank you to the committee members for your diligence. Thank you to the staff at the table here with me over the last two days.

The committee adjourned at 1141.

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