HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

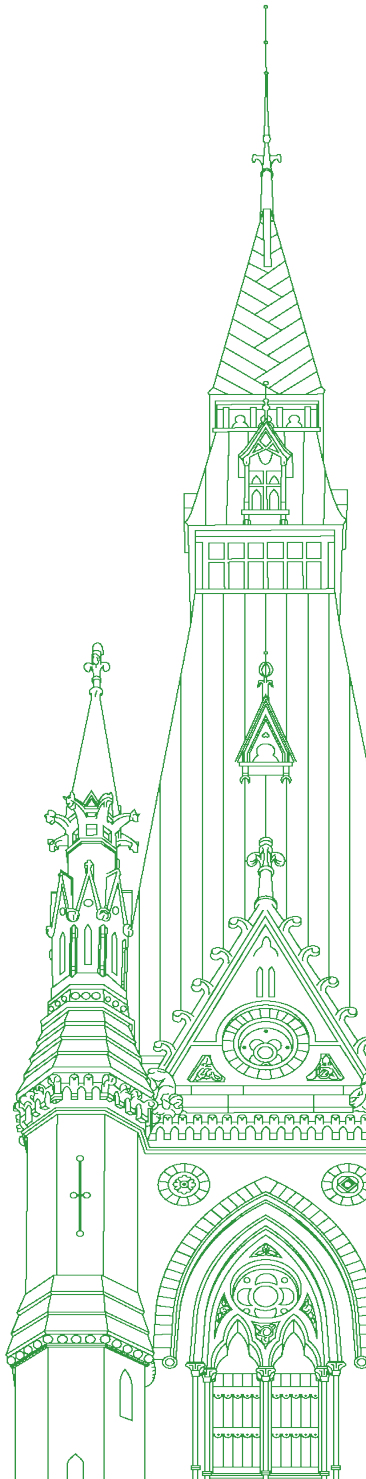
44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 094

Thursday, November 2, 2023



Chair: Mr. Joël Lightbound

Standing Committee on Industry and Technology

Thursday, November 2, 2023

● (1530)

[*Translation*]

The Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): Good afternoon, everyone. I call this meeting to order.

Welcome to meeting no. 94 of the House of Commons Standing Committee on Industry and Technology.

Today's meeting is taking place in a hybrid format, pursuant to the standing orders.

Pursuant to the order of reference of Monday, April 24, 2023, the committee is resuming consideration of Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.

I'd like to welcome our witnesses today: Daniel Konikoff, interim director of the Privacy, Technology & Surveillance program at the Canadian Civil Liberties Association; Tim McSorley, national coordinator at the International Civil Liberties Monitoring Group; Matthew Hatfield, executive director of OpenMedia; Sharon Polsky, president of the Privacy and Access Council of Canada; John Lawford, executive director and general counsel at the Public Interest Advocacy Centre, who is joined by staff lawyer Yuka Sai; and Sam Andrey, managing director of The Dais at Toronto Metropolitan University.

Thank you for being here today.

I'm pleased that we are able to start on time.

Without further ado, Mr. Konikoff from Canadian Civil Liberties Association, you have the floor for five minutes.

[*English*]

Mr. Daniel Konikoff (Interim Director of the Privacy, Technology & Surveillance program, Canadian Civil Liberties Association): Good afternoon. Thank you for inviting us to appear before you today.

I am the interim director of the privacy, technology and surveillance program at the Canadian Civil Liberties Association, an organization that has been standing up for the rights, civil liberties and fundamental freedoms of people in Canada since 1964.

Protecting privacy and human rights in our tech-driven present is no small undertaking. We commend the government for trying to modernize Canada's legislative framework for the digital age, and we commend the work that this committee is doing to get this legislation right.

We also acknowledge the procedural hurdles that may make it challenging for us to speak completely to Bill C-27 and its potential amendments. However, I will highlight three amendments from CCLA's written submission that we believe must be adopted to make Bill C-27 more respectful of people's rights in Canada.

First, Bill C-27 does not give fundamental rights their due and frequently puts them in second place, behind commercial interests. It has been said before but CCLA believes that it's worth emphasizing that Bill C-27 must be amended to recognize privacy as a human right, both in the CPPA and in AIDA, since privacy is something that should be respected at all points throughout data's life cycle.

This bill must also be amended to recognize our equality rights in the face of data discrimination and algorithmic bias, risks that grow exponentially as more and more data is gathered and fed into AI systems that make predictions or decisions of resounding consequence.

Privacy, data and AI legislation the world over, such as that in the European Union, already have stronger rights-based framing and protections. Canada simply needs to catch up.

Second, there are concerning gaps in Bill C-27 around the issue of sensitive information. Sensitivity is a concept that appears often throughout the CPPA; however, it is left undefined, allowing private interests to interpret its meaning as they see fit. A lot of personal information does qualify as sensitive, and although information's sensitivity often depends on context, there are special categories of information whose collection, use and disclosure carry inherent and extraordinary risks.

I want to draw your attention to one category in particular, the collection and use of which have implications for both the CPPA and AIDA, and that is biometric data.

Biometric data is perhaps the most vulnerable data we have, and its abuse can be particularly devastating to members of equity-seeking groups. Look no further than the prevalence of facial recognition technology. Facial recognition is used everywhere from law enforcement to shopping malls, and it relies on biometric information that is often collected without people's awareness and without people's consent. Right2YourFace coalition, of which CCLA is a member, has advocated having stronger legislative safeguards with respect to facial recognition and the sensitive biometric data that fuels it. Bill C-27 must be amended to not only explicitly define sensitive information and its many categories but also to unequivocally define biometric information as sensitive information worthy of special care and protection.

Third and finally, we take issue with the number of consent carve-outs in proposed section 18 of the CPPA, and how these can ultimately trickle down to AIDA. These carve-outs are, by and large, an affront to meaningful consent, and so to people's right to privacy. People should be able to meaningfully consent or decline to consent to how private companies gather and handle their personal data. Prioritizing a company's legitimate interest to violate consumer consent over people's privacy is simply inappropriate, as is leaving room for more consent carve-outs to be added in regulations later on. Bill C-27 is, frankly, porous with these exemptions and exceptions, and these gaps come at the expense of people's privacy.

There is no shortage of concerns around this bill, and I haven't really spoken to the issues that CCLA has with AIDA's narrow conception of harm, its lack of transparency requirements and its dangerous exclusions of national security institutions whose public mandates are often performed with privately acquired artificial intelligence technologies. We address these issues in greater depth in our written submission to the committee, but I'd be happy to expand on them in questioning.

I'd also like to direct the committee's attention to our written submission, which flags some of these concerns and includes an AI regulation petition that received over 8,000 signatures.

Bill C-27 overall needs tighter provisions to prioritize people's fundamental rights. The CPPA needs to plug its gaps around information sensitivity and consent, and if AIDA is not to be scrapped outright, reset or just separated from this bill, it needs fundamental rethinking.

Thank you.

● (1535)

The Chair: Thank you very much.

I'll now yield the floor to Mr. McSorley from the International Civil Liberties Monitoring Group.

Mr. Tim McSorley (National Coordinator, International Civil Liberties Monitoring Group): Thank you, Chair, and thank you for the invitation to share the perspectives of the ICLMG today regarding Bill C-27.

We're a Canadian coalition that works to defend civil liberties from the impact of national security and anti-terrorism laws. Our concerns regarding Bill C-27 are grounded in this mandate.

While we support efforts to modernize Canadian privacy laws and establish AI regulations, the bill unfortunately contains multiple exemptions for national security purposes that are unacceptable and undermine Bill C-27's stated goal of protecting the rights and privacy of people in Canada.

We have submitted a written brief to the committee with 10 recommendations and accompanying amendments. I'd be happy to speak in more detail about any of these during the question period, but for now, I'd like to make three specific points.

First, in regard to the CPPA, we are opposed to proposed sections 47 and 48 of the act, which create exceptions to consent by allowing an organization to disclose, collect or use personal information if it simply "suspects that the information relates to national security, the defence of Canada or the conduct of international affairs". This is an incredibly low threshold for circumventing consent.

Proposed section 48 is particularly egregious. It allows for an organization of "its own initiative" to collect, use or disclose an individual's personal information if it simply suspects that the information relates to these three areas. The concern does not even need to be connected to a suspected threat. Again, it only needs to relate, and that's not defined in the bill.

Not only are these sections very broad, they're also unnecessary. Other sections of the law would allow for more targeted disclosure to government departments, institutions and law enforcement agencies. For example, proposed section 45 allows an organization to proactively divulge information if it "has reasonable grounds to believe"—a much higher threshold—"that the information relates to a contravention" of a law that has been, is being or will be committed. We contrast that "reasonable grounds to believe" threshold with simply suspecting that it "relates".

In that regard, we find proposed sections 47 and 48 unnecessary and overly broad. We propose, then, that proposed sections 47 and 48 simply be removed from the CPPA. Barring that, we've proposed specific language in our brief that would help to establish a more robust threshold for disclosing personal information.

Second, we're deeply concerned with the artificial intelligence and data act overall. In line with other witnesses, we believe it is a deeply flawed piece of legislation that must be withdrawn in favour of a more considered and appropriate framework. We have outlined these concerns in our brief, as well as in a joint letter shared with the committee and the minister, signed by 45 organizations and experts in the fields of AI, civil liberties and human rights.

AIDA was developed without appropriate public consultation or debate. It fails to integrate appropriate human rights protections. It lacks fundamental definitions. Egregiously, it would create an AI and data commissioner operating at the discretion of the Minister of Innovation, resulting in a commissioner with no independence to enforce the provisions of AIDA, as weak as they may be.

Finally, I'd like to address an unacceptable exception for national security that is found in AIDA as well.

Canadian national security agencies have been open regarding their interest and use of artificial intelligence tools for a wide range of purposes, including for facial recognition, surveillance, border security and data analytics. However, no clear framework has been established to regulate the development or use of these tools in order to prevent serious harm.

AIDA should present an opportunity to address this gap. Instead, it does the opposite in proposed subsection 3(2), where it explicitly excludes the application of the act to:

> a product, service or activity that is under the direction or control of
>
> (a) the Minister of National Defence;
>
> (b) the Director of the Canadian Security Intelligence Service;
>
> (c) the Chief of the Communications Security Establishment; or
>
> (d) any other person who is responsible for a federal or provincial department or agency and who is prescribed by regulation.

This means that any AI system developed by a private sector actor that falls under the direction or control of this open-ended list of national security agencies would face absolutely no independent regulation or oversight.

It is inconceivable how such a broad exemption can be justified. Under such a rule, companies could create tools for our national security agencies without the need to undergo any assessment or mitigation for harm or bias, creating a human rights and civil liberties black hole. What if such technology were leaked, stolen or even sold to state or private entities outside of Canada's jurisdiction? All AI systems developed by the private sector must face regulation, regardless of their use by national security agencies.

Our brief includes specific examples of the harms that this lack of regulation can cause. I'd be happy to discuss these more with the committee. Overall, if AIDA does go ahead, we believe that proposed subsection 3(2) should simply be removed.

● (1540)

Thank you.

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

I'll now turn to Mr. Hatfield from OpenMedia, who is joining us by video conference.

Mr. Matthew Hatfield (Executive Director, OpenMedia): Good afternoon. I'm Matt Hatfield. I'm the executive director of OpenMedia, a grassroots community of nearly 300,000 people in Canada who work together for an open, accessible and surveillance-free Internet.

I'm speaking to you today from the unceded territory of the Tsawout, Saanich, Cowichan and Chemainus nations.

What is there to say about Bill C-27? One part is long-overdue privacy reform, and your task is closing its remaining loopholes and getting the job of protecting our data done. One part is frankly undercooked AI regulation that you should take out of Bill C-27 altogether and take your time to get right. I can't address both at the length they deserve. I shouldn't have to, but we are where the government has forced us to be, so let's talk privacy.

There are some great changes in Bill C-27. These include real penalty powers for the OPC and the minister's promised amendments to entrench privacy as a human right. OpenMedia hopes this change to PIPEDA will clearly signal to the courts that our ownership of our personal data is more important than a corporation's interest in profiting off that data, but any regulatory regime is only as strong as its weakest link. It does no good for Canada to promise the toughest penalties in the world if they're easy to evade in most real-world cases. The weaknesses of Bill C-27 will absolutely be searched for and attacked by companies wishing to do Canadians harm.

That's why it's critical that you remove the consent exceptions in Bill C-27 and give Canadians the right to ongoing, informed and withdrawable consent for all use of our data. While you're fixing consent, you must also broaden Bill C-27's data rules to apply to every non-governmental body. This includes political parties, nonprofit organizations like OpenMedia and vendors that sell data tools to any government body. No other advanced democracy tolerates a special exception to respecting privacy rules for the same parties that write privacy law. That's an embarrassing Canada original, and it shouldn't survive your scrutiny of this bill.

Privacy was the happier side of my comments on Bill C-27. Let's talk AI.

I promise you that our community understands the urgency to put some rules in place on AI. Earlier this year, OpenMedia asked our community what they hoped for and were worried about with generative AI. Thousands of people weighed in and told us they believe this is a huge moment for society. Almost 80% think this is bigger than the smart phone, and one in three of us thinks it will be as big or bigger than the Internet itself. “Bigger than the Internet” is the kind of thing you're going to want to get right, but being first to regulate is a very different thing from regulating right.

Minister Champagne is at the U.K.'s AI safety conference this week, telling media the risk is in doing too little, not too much. However, at the same conference, Rishi Sunak used his time to warn that we need to understand the impact of AI systems far more than we currently do, in order to regulate them effectively, and that no regulation will succeed if countries hosting AI developments do not develop their standards in close parallel. That's why the participants of that conference are working through foundational questions about exactly what is at stake and in scope right now. It's an important, necessary project, and I wish them all success with it.

If they're doing that work there, why are we here? Why has this committee been tasked with jamming AIDA through within a critical but unrelated bill? Why is Canada confident that we know more than our peers about how to regulate AI—so confident that we're skipping the basic public consultation that even moderately important legislation normally receives?

I have to ask this: Is AIDA about protecting Canadians, or is it about creating a permissive environment for shady AI development? If we legislate AI first, without learning in tandem with larger and more cautious jurisdictions, we're not going to wind up with the best protections. Instead, we're positioning Canada as a kind of AI dumping ground, where business practices that are not permitted in the U.S. or the EU can be produced here in rights-violating and even dangerous ways. I'm worried that this is not a bug, but rather the point—that our innovation ministry is fast-tracking this legislation precisely to guarantee Canada will have lower AI safety standards than our peers.

If generative AI is a hype cycle whose products will mostly underwhelm, then this is much ado about not much and there is no need to rush the legislation. However, if even a fraction of it is as powerful as its proponents claim, failing to work with experts and our global peers on best-in-class AI legislation is a tremendous mistake.

I urge you to separate AIDA from Bill C-27 and send it back for a full public consultation. If that isn't in your power, at the very least, you cannot allow Canada to become an AI dumping ground. That's why I urge you to make the AI commissioner report directly to you, our Parliament, not to ISED. A ministry whose mandate is to sponsor AI will have a strong temptation to look the other way on shady practices. The commissioner should be charged with reporting to you yearly on the performance of AIDA and on gaps that have been revealed in it. I also urge you to mandate parliamentary review of AIDA within two years of Bill C-27's taking effect, in order to decide whether it must be amended or replaced.

Since PIPEDA reform was first proposed in 2021, OpenMedia's community has sent more than 24,000 messages to our MPs demanding urgent comprehensive privacy protections. In the last few months, we've sent another 4,000 messages asking our Parliament to take the due time to get AIDA right. I hope you will hear us on both points.

● (1545)

Thank you, and I look forward to your questions.

[*Translation*]

The Chair: Thank you.

Now to hear from Ms. Polsky, from the Privacy and Access Council of Canada.

[*English*]

Ms. Sharon Polsky (President, Privacy and Access Council of Canada): Thank you.

Thank you for inviting me to share some views about Bill C-27 on behalf of the Privacy and Access Council of Canada, an independent, non-profit and non-partisan organization that is not funded by government or by industry.

Our members in public, private and non-profit sector organizations work with and assess new technologies every day, as have I through my 30-plus-year career as a privacy adviser. For that entire time, we have all heard the same promise: Technology will provide great benefits. To an extent, it has.

We’ve also been nudged to do everything digitally, and data is now the foundation of many organizations that collect, analyze and monetize data, often without the knowledge, much less the real consent, of the people the data is about.

It's understandable that there's great support for Bill C-27, except that many of the people who support it don't like it. They figure, though, that it's taken 20 years to get this much, and we can't wait another 20 for something better to replace PIPEDA, so it's better than nothing at all.

With respect, we disagree. We do not share the view that settling for the sake of change is better than standing firm for a law that, at its heart, would definitively state that Canadians have a fundamental right to privacy. The minister's concession to add that into the bill itself and not just the preamble is very welcome.

We disagree that settling for bad law is better than nothing, and Bill C-27 is bad law because it would undermine everyone's privacy, including children's—however they're defined in each jurisdiction. It also does nothing to counter the content regulation laws that would undermine encryption, would criminalize children who try to report abuse and would make it impossible for even your private communications to be confidential, whether you consent or not.

Definition determines outcomes, and Bill C-27 starts off by defining us all as "consumers" and not as individuals with a fundamental human right to privacy. It promotes data sharing to foster commerce, jobs and taxes. It adds a new bureaucracy that would be novel among data protection authorities and would delay individuals' recourse by years. It does not require AI transparency or restrict AI use by governments, only by the private sector that has not yet been deputized by government, which then gets sheltered by our current ATIP laws.

It won't slow AI and facial recognition from infiltrating our lives further. It won't slow the monetization of our personal information by a global data broker industry already worth more than $300 billion U.S. It doesn't impose any privacy obligations on political parties. It doesn't allow for executives to be fined—only organizations that then include the fine as a line item in their financials and move on, happy that their tax liabilities have been reduced.

Bill C-27 does allow personal information to be used for research but by whom or where in the world isn't limited. Big pharma using your DNA to research new medicines without your consent is just fine if it's been de-identified, although it can be easily reidentified, and larger and larger AI datasets make that more and more likely every day.

Bill C-27 would require privacy policies to be in plain language, and that would be great if it stated the degree of granularity required, but it doesn't. It allows the same vague language and generalities we now have, yet it still doesn't allow you to control what data about you may be shared or with whom, or give you a way to be forgotten.

It lets organizations collect whatever personal information they can from you and about you, without consent, as long as they say, in their self-interested way, that it's to make sure nothing about you is a threat to their "information, system or network security", or if they say the collection and use "outweighs any potential adverse effect" on you resulting from that collection or use, and leaves it to you to find out about and to challenge that claim.

We've all heard industry's threat that regulation will hamper innovation. That red herring was invalidated when radio didn't kill newspapers, TV didn't kill radio and the Internet didn't kill either one. Industry adapted and innovated, and tech companies already do that with each new product, update and patch.

Companies that have skirted the edge of privacy compliance can adapt and innovate and can create things that, at their core, have a genuine respect for privacy, human rights, and sound ethics and morality. They can, but in almost a half a century since computers landed on desktops, most haven't. Politely asking organizations to consider the special interests of minors is lovely but hardly compelling, considering that, 20 years after PIPEDA came into force, barely more than half of Canadian companies the OPC surveyed have privacy policies or have even designated someone to be responsible for privacy.

● (1550)

Those are basic and fundamental components of a privacy management program that do not take 20 years to figure out. We don't have time to wait, but we also cannot afford legislation that is inadequate before it's proclaimed, that's not aligned with Quebec's Law 25, the U.S. executive order on AI or other jurisdictions that are well ahead of Canada on this. We also can't afford something that further erodes trust in government and industry as it freely trades away the privacy rights of Canadians for the sake of commercial gain.

I will be happy to answer your questions, and we will be detailing our views in a submission to the committee. I hope you hear us.

● (1555)

[*Translation*]

The Chair: Thank you very much.

I'll now give the floor to Mr. Lawford and Ms. Sai from the Public Interest Advocacy Centre.

[*English*]

Mr. John Lawford (Executive Director and General Counsel, Public Interest Advocacy Centre): Thank you, Chair.

The Public Interest Advocacy Centre is a national, non-profit and registered charity that provides legal and research services on behalf of consumers—in particular, vulnerable consumers. PIAC has been active in the field of consumer privacy law and policy for over 25 years.

My name is John Lawford. I'm the executive director and general counsel. With me today is Yuka Sai, staff lawyer at PIAC.

Bill C-27 reverses 25 years of privacy law in Canada. Businesses can now assume consent, and consumers must prove abuse. If this sounds uncomfortable from an individual rights perspective, that's because it is.

Firstly, with regard to consent, the new business activities exception to consent, which is in proposed subsection 18(1), makes full use of your personal information without your consent, or even your knowledge, legal for business. Business activities are defined so widely and tautologically in proposed subsection 18(2) that only businesses will be able to define what a business is. It's ridiculous. Proposed section 18 completely reverses the default of an individual's informed consent for the collection or use of personal information under PIPEDA. Do Canadians really want that?

The addition of an exception to consent and knowledge in proposed subsection 18(3), for the collection or use of additional personal information for legitimate interests, is an import from European law but without the fundamental right to privacy that it modulates in Europe.

Secondly, with regard to de-identification, under proposed section 20, consumers also lose out on opportunities to scrutinize the use of their personal information when it is de-identified. De-identify is defined as:

> to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains.

It is akin to saying that to kill means to take the life of a person directly, although a chance of their remaining alive remains. It is contradictory and meaningless.

De-identification was also clearly a “use” of personal information under PIPEDA. What that use approach stops is the indiscriminate filling of databases with personal information with only the most cursory removal of tombstone information identifiers from the data. Reidentification is therefore a real risk, but even de-identified information can harm individuals when they are profiled in databases that are then used to market to them or to deny them services. Bill C-27 supercharges this outcome.

Go ahead, Yuka.

Mrs. Yuka Sai (Staff Lawyer, Public Interest Advocacy Centre): Proposed section 39 facilitates a pipeline of data between the industry and the public sector. The government can prescribe any purpose or public entity as “socially beneficial” and consumers would never know to question it until issues emerge. We remind everyone of Telus giving PHAC cellphone data information in 2021.

Artificial intelligence, AI, simply is rocket fuel for discrimination. The AIDA portion of this bill lacks substance on bias, systemic harms, high impact systems and government applicability, and denies independent oversight.

The proposed tribunal is purpose-built to kill enforcement of the new act. It enables businesses to prolong the resolution process with a soon-to-be captured review board akin to the Competition Tribunal. It delays to the point of death any class action. The Privacy Commissioner, instead, should have the power to issue orders and penalties, with decisions subject to appeal before the Federal Court.

Mr. John Lawford: On EU adequacy, unless the EU really looks the other way, any law in this mould certainly will be inadequate for European adequacy.

In conclusion, this bill should be wholly rejected. Consumers are infinitely better protected under PIPEDA. The bill is a deliberate attempt to grease the rails for business and for AI.

These are our thoughts. Thank you very much, and we look forward to your questions.

The Chair: Thank you very much.

I'll now turn to Sam Andrey, managing director of the The Dais, Toronto Metropolitan University.

● (1600)

Mr. Sam Andrey (Managing Director, The Dais, Toronto Metropolitan University): Thank you for the invitation to address the committee today.

I'm Sam Andrey. I'm the managing director of the Dais, a think tank at Toronto Metropolitan University where we work to develop the policy ideas to advance an inclusive, innovative economy, education system and democracy for Canada.

I'm going to focus my remarks today on the AI and data act. As many of my colleagues have noted, AI has the potential to have a transformative impact on our economy and our daily lives, but it also poses significant risks, including systemic forms of discrimination, psychological harms and malicious use.

The latest data from StatsCan shows that only about 4% of Canadian businesses are using AI, so to reach AI's full potential and increase adoption, we need a responsible governance framework.

Unfortunately, we think the current bill fails to adequately do that. The bill's surprise introduction and lack of public consultation since have limited the ability of folks in civil society, experts, industry and equity-deserving communities to engage with this important legislation. Our team at TMU, led by Christelle Tessono, has partnered with McGill University's Centre for Media, Technology and Democracy to engage with many of these folks over the last year and has produced recommendations for improving the bill, which we'll be sending to the committee.

I'm just going to highlight three of those today that we hope can be addressed if AIDA is moving forward.

First, the bill's definition of “harm” is very narrowly focused on individuals, but the harms of AI systems also occur at broader community and group levels. Depending on the type and context of the system in question, harm to individuals can be difficult to prove and only evident when assessed at a population level. Moreover, there are types of collective harms that are manipulative and exploitative from AI that would likely not be captured by this definition. Things like election interference, harm to the environment and collective harms to children are not harms that would be captured by the definition, which is focused on individuals.

Second, as my colleagues have said, the proposed regulatory model does not create sufficient independence from the minister of ISED, who would have competing roles of championing the economic benefits of AI while regulating and enforcing its risks. We think that the proposed AI and data commissioner needs to be independent from the minister, ideally through a parliamentary appointment and certainly with sufficient resources to support their role.

We would also propose two additions. One is the ability for individuals to make complaints to the commissioner. Currently to launch any investigation, the minister has to have reasonable grounds to believe that an investigation is warranted, which is a very high bar. The other is for the commissioner to be able to conduct pre-emptive audits.

Third, as has been mentioned, this bill currently only applies to the private sector. Minister Champagne's proposed list of high impact systems that he's shared with this committee that would be potentially subject to regulation includes a number of AI systems commonly used by public sector actors, like facial recognition used by the police and health care, but it creates a double standard where the private sector developers of these systems are going to be subject to regulation and our public servants operating them will not be.

This double standard is unlike the EU, and it fails to position the Canadian government as leading by example through legal bans and guardrails for its own responsible development and use of AI. The current structure of the bill, particularly its commissioner being an ISED departmental official, makes it poorly structured to provide oversight for all public sector AI. We acknowledge that it would not be an easy amendment job, but I would just note that Parliament needs to prioritize the development of AI regulation for the public sector, which needs to include adequate public consultation and engagement.

I want to close by saying that Canada's investments in developing AI systems and research have not yet been matched by a comparable effort to regulate the quickly evolving risks of the technology. We're encouraged that the minister and this committee are open to amendments that will strengthen the bill, and there's really a large community across Canada who wants to help.

Thank you for the opportunity.

[*Translation*]

The Chair: Thank you very much.

To get discussion started, I'm going to give the floor to Mr. Perkins for six minutes.

[*English*]

Mr. Rick Perkins (South Shore—St. Margarets, CPC): Thank you, Mr. Chair.

Thank you, witnesses, for your excellent presentations on this important bill.

In the first few meetings, my colleagues on the government side were probably sick of hearing me say that it's a broken bill, but it is a broken bill in the—

Mr. Tony Van Bynen (Newmarket—Aurora, Lib.): I'm on the English channel and getting French.

The Chair: Hold on for one second. We'll make sure that everything is working properly.

● (1605)

Mr. Tony Van Bynen: It's working now. Thank you.

[*Translation*]

The Chair: Okay, that's perfect.

Mr. Perkins, you can start from the beginning.

[*English*]

Mr. Rick Perkins: I'll start from the beginning.

Thank you for coming and for your excellent presentations on this important bill.

In the first number of meetings, we were calling this bill a broken bill for a lot of the reasons that all of you outlined. You've probably been following it.

The fundamental right in the purpose clause is critical from our perspective. It's certainly critical that, in the purpose section, it is at a level of superiority to the need of an organization's ability to use it.

Perhaps I could start off by asking Mr. Konikoff if he believes that the words there need to be not personal privacy and an organization's right, but some other language that makes it superior to that.

Mr. Daniel Konikoff: At present, my gripe would be with the lack of extension of the fundamental right to privacy to AIDA. I'd say that is really the biggest weak spot with regard to this. We commend the minister for including that in his proposed amendment.

As for the language, I'd need to take a moment to review that, but I'd say that perhaps the most concerning piece is the fact that it doesn't essentially trickle down from the CPPA to AIDA.

I'd happily defer to anyone else on this panel if they have any—

Mr. Rick Perkins: I will move on then to Mr. Lawford.

One thing that's come up recently about the issues.... I've spoken a lot about the issues of proposed sections 12, 15 and 18, which you outlined. Proposed section 15 outlines plain language in consent, which obviously is not something we get a lot of when we do that.

I'm reading the latest terms and conditions from Zoom, which were released in the summer. It reached the news that Zoom was actually taking the right to transcribe and own everything that is said.

The thing that really bothers me is 15.2 of their terms and conditions, which is in almost every organization. It says, "You agree that Zoom may modify, delete, and make additions to its guides, statements, policies, and notices, with or without notice to you, and for similar guides, statements, policies, and notices applicable to your use of the Services by posting an updated version on the...webpage." They don't actually come out and say that, if they're changing the terms, they'll just post it somewhere on a mysterious web page and assume that you've consented to the fact that they're now going to transcribe and own everything you say on Zoom.

I'll leave proposed section 18 because that's a different discussion, but what can be done in proposed section 15 to fix that so that companies don't have the right to do whatever they want to the terms and conditions without an individual's knowledge?

Mr. John Lawford: Under the present act, if you change the purpose for which you're using and collecting personal information, you have to give a chance for reconsent. The Privacy Commissioner hasn't always received complaints on that type of approach, but at the moment at least, you could complain that the initial consent was based on a different set of terms and conditions. If they want to change the terms and conditions, especially if it's just posting and all you do is use it to accept them, then at least at the moment you could do that.

My concern is with proposed section 18. Zoom can say that it's the way business is done with online programs now, so you have to complain to the Privacy Commissioner. That's why I've said this reverses the onus from the present law, where consent has to be sought. You could change this bill to require new consent when the purposes have changed. That could go in proposed section 15 for certain—

Mr. Rick Perkins: In other words, it's not there. There's nothing in Bill C-27 that prevents this practice from continuing, where a business says it's changing the current terms and conditions of consent and complying with the law by posting it. If anyone challenges it, even though they'll never discover it because they don't know it happened, the business can go through a process to appeal and under the CPPA's proposed subsection 18(3) in particular, it can say, "Too bad. We have the right because it's in our business's legitimate interest to do so."

Mr. John Lawford: If you brought a complaint, the business would probably raise that as one of its defences. I would think that it would also rely on proposed subsection 18(2) of the CPPA and say, "That's the way business is done in this business, and good luck with your complaint." Taking out proposed section 18 completely would be our recommendation.

● (1610)

Mr. Rick Perkins: You mean all of proposed section 18, not just subsection 18(3).

Mr. John Lawford: Yes, I mean the whole thing.

Mr. Rick Perkins: Would anyone else like to comment on that particular issue?

Ms. Polsky.

Ms. Sharon Polsky: Thank you.

Yes, the issue of consent has been a challenge the whole time. Even under PIPEDA and other privacy laws, an organization is not supposed to be able to refuse to provide the good or service just because you refuse to provide consent. However, they all do, and that hasn't been challenged and hasn't been enforced. As you say, with regard to Zoom and all the rest of them, they do collect the information.

We don't have a choice right now. It's all or nothing, a Faustian bargain. If you want to use this website, if you want to get a car loan online, if you want to do anything online, yes, you're supposed to read the privacy policy that Mark Zuckerberg also admitted to Congress even he doesn't read. Therefore, the organizations—that acknowledge that no one reads their privacy policies and that, yet, still collect the personal information without now, admittedly, having received informed consent—are collecting personal information in violation of PIPEDA and the other laws. No one's ever challenged that.

The only way we're going to get around it is to give each one of us a control as to who gets our information and what they're going to do with it. If I say, "Yes, Zoom, you may collect these pieces of information about me, and you will give me a receipt, an automated receipt system, so that I have proof that this is what I consented to," then I have something to challenge it with. If the companies were held to account.... It's a challenge because most of them are outside of Canada, but other laws do have extraterritorial reach. Perhaps this one could as well, because consent is the foundation of all of this. In the EU also, it's not a whole lot better. That's one that we absolutely have to tighten up.

Mr. Rick Perkins: Most privacy lawyers that I've talked to in my consultation on this—and I've done a lot of consultation on this, contrary to what the minister did—have said that they don't even read the consent requirements that they're asked to do. If privacy lawyers don't do it, how are the rest of us going to survive?

The Chair: Thank you, Mr. Perkins.

Mr. Van Bynen, the floor is yours.

Mr. Tony Van Bynen: Thank you, Mr. Chair.

I understand the concerns that you have in terms of requiring consent. How are you going to deal with consent fatigue? Is that a risk that you...?

I'll start with Mr. Konikoff.

Mr. Daniel Konikoff: I personally don't think that consent should be something that we can be fatigued of. I think that consent is an ongoing process and something where, regardless of a service, the more informed you are at the outset before using it.... I recognize that there are challenges in place or that there are hurdles to getting people to actually meaningfully engage with very boring, very stuffy privacy policies. I don't think that it's really something I would conceive in terms of fatigue.

Mr. Tony Van Bynen: However, isn't that what's happening now? The complexity of the consent means that people don't read them, but people provide it. It's enabling organizations to deal with their data in any way they wish. It's an offshoot of consent fatigue. How do we get around that? How do we develop, perhaps, plain language consent?

Ms. Polsky, you had a suggestion around providing consent in advance of.... Could you explain that a little further, please?

Ms. Sharon Polsky: Consent fatigue I don't think is a problem. As you say, people don't read these things, first of all, because the last time I counted.... I do read them sometimes—or often. The last time I counted, for Google and its primary websites, the combined length of the privacy policies was 38 pages. It's a small book. It's bigger than a bedtime book, and it puts you to sleep faster. They're meaningless.

I challenged the Apple privacy policy to the Privacy Commissioner of Canada. He took it up, which was great. They changed some language, and that was wonderful. However, I'm under no illusions. When they change something here, they change something else there. The problem is that the law allows vague language such as “We will collect your personal information from you and about you for reasonable purposes. We are a for-profit business. Anything that improves our bottom line we think is a reasonable purpose.” It needs to be tightened up.

● (1615)

Mr. Tony Van Bynen: Thank you.

Mr. Konikoff, in your brief to the committee, you recommended deleting proposed paragraph 18(2)(d) in the consumer privacy protection act, which provides an exception to consent for “any other prescribed activity.”

Conversely, in the brief of the Office of the Privacy Commissioner of Canada on Bill C-27, the Privacy Commissioner recommends amending this provision to require that all prescribed business activities for the purposes of proposed subsection 18(2) be activities necessary to achieve a specific purpose. What do you think of the Privacy Commissioner's recommendation?

Mr. Daniel Konikoff: This is a great question.

All I know is that by leaving that language in there for any “prescribed activity”, I fear that there's too wide a catch-all. I think the language is frustratingly vague, and I worry that, without any sort of clear definition on what any prescribed activity is, that could be very much ripe for abuse. Whether that means you take that out or you provide some sort of clearer restriction on activities, I feel that there shouldn't be these large carve-outs that allow any prescribed activity to be added later on.

Mr. Tony Van Bynen: What value do you place on the requirement for impact assessments?

Mr. Daniel Konikoff: I think that, if you are using a system that will be gathering some sort of high volume of data, a privacy impact assessment is a good first step in terms of making sure that you're doing the due diligence, getting out ahead of this and assessing potential risks.

Mr. Tony Van Bynen: The reality is that the genie is out of the bottle.

We're using Interac. We're using AI, and you're saying, “Slow down and start over again.” What type of a time window, a timeline, would you put on that so that we catch up to—if not get ahead of—where the industry is now?

Mr. Daniel Konikoff: It's not my job to really put a timeline on anything, nor do I really understand how these processes work. It seems to me that it takes quite a while.

Again, it's not about starting over on the CPPA, I wouldn't say. It's about starting over on AIDA or about separating AIDA—or at least making some sort of decision around what to do with AIDA—which it seems most are in agreement is difficult, with “difficult” being an understatement. I don't know if I can speak exactly to the timeline question.

Mr. Tony Van Bynen: I guess my concern is that we're in catch-up now. How are we ever going to catch up or even get ahead of the situation? Legislation seems to be focused on the rearview mirror when we should be looking out the windshield. I think it's important. Where would we get an understanding of what the timelines are to develop the sense of urgency in going forward with at least the AIDA?

Mr. Daniel Konikoff: With AIDA...? Again, I assume it would have to do with the machinations of government. I assume that it would have to do with sending the bill back. That's within your power, I believe. Matt stated that it's within your power. It is a possibility.

I think it's something that would need more.... Matt is on the screen over there, so that would be something that perhaps.... I don't know if I could speak to timelines.

Mr. Tony Van Bynen: Mr. McSorley, it seems that you might have a response there, so let's hear it.

Mr. Tim McSorley: Yes. One of the things we've noted is that the minister, I believe, has said that, even for the development of regulations, it should take until 2025 to have all the regulations sorted out for AIDA in its current form. If that's the timeline we're looking at with AIDA in its current form, that should give us time to also step back, look at AIDA overall and engage in that reset my colleague has been speaking about.

We agree that we need to be addressing these issues now, but if already in the way that AIDA is currently envisioned it's going to take that time, why not take that time to also engage in broader consultation, do the public consultation that didn't happen before AIDA was introduced and make sure we get it right by then?

Mr. Tony Van Bynen: Thank you.

I must be out of time, Chair.

The Chair: You are, but I see that Mr. Hatfield wanted to intervene.

You have the floor, Mr. Hatfield.

Mr. Matthew Hatfield: Thank you.

Speaking to the point of urgency, like I said, our community also feels some urgency, but why is the urgency so much higher in Canada than in other jurisdictions that are looking at AI? Everyone is moving forward, of course, with delineating the risks, the impacts and how to address them appropriately, but the idea that Canada must move before many of our peers doesn't make a lot of sense to me. I don't think it's going to lead to the best possible rules.

I think that, if we're looking at the timeline, at the very least we should be taking the time for a full public consultation. Consultations like that are really how we stress-test legislation and tease out the different types of problems that can occur. It's a really critical step to improving the final product. We've seen it work with other legislation. It's done on most legislation. I don't see any good reason why we skipped it here.

● (1620)

[*Translation*]

The Chair: Thank you very much.

Mr. Savard-Tremblay, the floor is yours.

Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ): Thank you, Mr. Chair.

I'd like to thank the committee for having me here today, even though it's not a committee I usually sit on. It's a pleasure to be here.

I want to thank the witnesses for their presentations.

Mr Konikoff, if you don't mind, I'd like to talk about automated decision systems. As we know, Bill C-27 grants a new right, namely the right for an individual to receive an explanation about the use of these systems. However, unlike Quebec's Bill 25, Bill C-27 does not contain provisions that would allow a person to object to the use of an automated decision system or to have a review of the decisions made by such a system.

In your opinion, what are the potential repercussions for consumers and users if Bill C-27 does not include such provisions?

[*English*]

Mr. Daniel Konikoff: That is a great question.

There are tremendous implications for not having these transparency requirements. You mentioned Quebec, but I can also turn to the GDPR, which is not explicitly to do with AI but has implications for AI, what with the use of data in AI. The GDPR contains a right within it that is the right to not be subject to a decision based solely on automated systems. I think that is something that could potentially serve as a template to be included in AIDA, as well as clearer transparency requirements not only for systems that are high impact, but for systems that are....

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: You would therefore be in favour of adding provisions to Bill C-27, provisions similar to those adopted in Europe and Quebec.

[*English*]

Mr. Daniel Konikoff: Yes.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: According to Bill C-27 as it currently stands, who should consumers turn to if they want to contest a decision made by an automated system or obtain clarification about that decision?

[*English*]

Mr. Daniel Konikoff: I beg your pardon. Can you repeat that?

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: According to Bill C-27 in its current form, who should consumers turn to if they want to contest a decision made by an automated system? Is there a body, organization or authority they can turn to?

[*English*]

Mr. Daniel Konikoff: No. I don't think so. There is a consumer challenge.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: Would anyone else like to add anything?

[*English*]

Mr. Sam Andrey: Yes. If it has a significant impact, you have the ability to request information, but there is no ability to appeal, challenge or have a human review it, as you say other jurisdictions have done.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: So that's a problem, in your view.

[*English*]

Mr. Sam Andrey: Yes.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: Mr. Konikoff, what do you think is preventing us from making both the public and private sectors subject to the provisions of the bill? Do we need to go further to ensure data belonging to Quebeckers and Canadians is protected?

[*English*]

Mr. Daniel Konikoff: We go further to protect information. Yes, I absolutely don't think this goes far enough. We've laid out some possibilities to firm that up.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: Mr. McSorley, as you know, last month, the Minister of Innovation, Science and Industry presented a voluntary code of conduct for responsible development and management of advanced generative AI systems.

At a time when technologies are evolving rapidly, is self-regulation the best solution? Do you think it's realistic to think that companies, guided by some invisible hand, will simply regulate themselves?

[*English*]

Mr. Tim McSorley: Very simply, no. Self-regulation is not appropriate or adequate.

I think this is a clear example of what my colleague Mr. Hatfield was saying around the idea of rushing to regulate, rather than really understanding the system. The entire consultation process around regulating generative AI was done in such a rushed manner. We felt a response to concerns that there hadn't been public consultation about AIDA in general. We have concerns.

We don't have any data right now to know how companies are reacting to the self-regulation, but it's clearly insufficient.

● (1625)

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: Ms. Polsky, in a document dated April 14, 2023, the Privacy and Access Council of Canada states that the AI legislation being proposed by the European Union will likely become the global standard for general-purpose generative AI systems.

Why do you think the law being proposed by the European Union could become the global standard?

[*English*]

Ms. Sharon Polsky: We have seen with the GDPR that the comprehensiveness of that regulation and its extrajurisdictional applicability became the global standard very quickly. It was a bar that was set high. Yes, a lot of organizations and a lot of companies whined and complained and said that it was going to cost them a lot of money to comply with the law, and they did it anyhow.

We can see the same thing if Canada takes an approach for AI regulation for privacy that has teeth.

I remember when Jennifer Stoddart declined to be reappointed, and she said that PIPEDA could use a little more teeth. That was tough talk. PIPEDA needs it. We can do it, but there needs to be political will.

[*Translation*]

The Chair: Thank you very much.

I'll now give the floor to Mr. Masse.

[*English*]

Mr. Brian Masse (Windsor West, NDP): Thank you, Mr. Chair.

Thank you to our witnesses.

I will start with Mr. Lawford. If others are...I will check in.

In particular, I'm curious about your view of the privacy tribunal. I'm hearing what you're saying in terms of the overall message, but at the same time, if there was progress on some of these elements.... The one new factor is the new privacy tribunal, and there are those who are for and against it. We would love to have your opinion to start.

Mr. John Lawford: We base our opposition to this on the fact that the Privacy Commissioner presently does investigations and, although they are sometimes slow, the results are, in our opinion, fair.

We looked at the Competition Tribunal debacle this year with Rogers and Shaw, and the use of that extra step, if you will, by a company that felt like dragging out a process or winning.... We can't see any likelihood that companies using personal information won't take that extra step and go to the tribunal to challenge every commissioner decision. That very likely adds two years to all negative decisions on companies' parts. You could say that presently you can go from the Privacy Commissioner's decision to the Federal Court, but you have to re-prove the case in front of the Federal Court.

It seems like an unnecessary step. When you add that along with our concerns that you can't bring a class action until after all the proceedings are done, including in front of the tribunal, that will discourage class actions. We believe that some private enforcement does change the behaviour of companies when there are egregious privacy violations.

Our concern is that this is just setting up a structure that is an extra step and may well be less favourable to complainants like the Competition Tribunal is to the competition commissioner.

Mr. Brian Masse: Yes. On that, officials said to me that it couldn't happen under this act. Then we have had other testimonies saying that it could happen. What's your opinion on that?

That case against the Competition Bureau is nothing short of outrageous. It undermines the whole point of the Competition Bureau and basically has the public subsidizing Rogers in many different ways. At any rate, what's your take on that possibility?

Mr. John Lawford: We have a lot of concerns about that, especially since the initial draft of what the privacy tribunal would be like would be that there would be only one privacy expert on that.

The Privacy Commissioner presently has enough expertise to make a proper administrative decision, and then we have courts, if you want to go and say there's a problem above that. That's a much more efficient way, and it's a more predictable way to deal with this rather than creating a quasi court. Quasi courts tend to have quasi judges on them, and you get quasi decisions like we had with Rogers, so we would prefer to avoid that.

● (1630)

Mr. Brian Masse: I'm not aware of any other country that has a privacy tribunal.

One thing I would like to ask before I turn it over to some other guests is this: What's your view on the private right of action that the United States has? What's the importance of that versus what we don't have here?

Mr. John Lawford: In the United States, of course, they don't have a comprehensive privacy law. We're lucky to have PIPEDA here, so a lot of our issues don't have to go to court. However, for those very difficult situations or widespread privacy violations, at least the threat of a class action can focus the minds of the larger corporations. We think that it's a good tool to use and to preserve in this act.

I will just say that, for PIPEDA, there was a private right of action with an amount per privacy violation, which was never proclaimed into force because of lobbying from the industry. It could have been better these last few years, but keeping that possibility open is a concern of ours—yes.

Mr. Brian Masse: Ironically, in Canada, we actually benefit from some of those class actions in the United States while we can't do them here. Canadians are actually protected under U.S. law to be involved in some of the reimbursements in the United States. There are several cases where we have to notify Canadians about them. They actually protect Canadians better than our current system.

Is there anyone else who would like to talk about the privacy tribunal? Even if you have a different opinion, I'm interested in hearing you. If you don't want to jump in at the moment, I'll move to another question.

Ms. Sharon Polsky: I will offer a quick comment. There is some concern as to who will be appointed and by whom. If there's only going to be one privacy expert on the tribunal, who is appointed by the industry ministry, whose interest is to promote commerce, it undermines fairness. We also are concerned, though, that if a commissioner's decision ends up having to be reviewed, and then the offending organization has the opportunity to exhaust all of its legal recourse—as Mr. Lawford said— that this creates delay.

Then a private right of action kicks in. I now get the honour and pleasure to hire a lawyer and spend even more money and more years, with the offending organization having much deeper pockets than most people, I would venture. Up to what point...? By the time they have exhausted their legal recourse, am I even going to be alive?

Mr. Brian Masse: Thank you, Mr. Chair.

Thank you to the witnesses.

The Chair: Thank you very much.

Mr. Williams.

Mr. Ryan Williams (Bay of Quinte, CPC): I'd like to talk about AIDA, the AI act, with each one of you. I'm going to ask each one of you and give you some time to answer.

On a scale of one to 10, one being terrible and 10 being good, how good or how bad is this AIDA legislation in this part of the bill right now?

I'll start with Mr. Konikoff.

Mr. Daniel Konikoff: Oh, my God! Do we have to pick a number? Should we try to get on board together with what numbers we're going to go for here?

Voices: Oh, oh!

Mr. Daniel Konikoff: I would rate it south of five, if I'm being generous, although I don't know where we're at. Given our mandate to look at fundamental rights and privacy, it is a failure on both fronts. Maybe five is high.

Mr. Ryan Williams: Mr. McSorley...?

Mr. Tim McSorley: I give it a two.

Mr. Daniel Konikoff: Do you know what? I'm going to go with two.

Voices: Oh, oh!

Mr. Ryan Williams: That changed back.

Ms. Sharon Polsky: I think you're being very generous at five.

It's a starting point. It has drawn attention. It has turned your minds, and the discussions have turned your minds to some of the very many problems that have to be faced. As a starting point...yes, okay. As to what it is now, I'd say about a one—generously a one and half.

Mr. Ryan Williams: Mr. Lawford...?

Mr. John Lawford: I think together we each give it a one—so two.

Mr. Sam Andrey: Maybe a three.... I may be more charitable, but I think it was well intended. I don't ascribe malicious motives to it, but it has a lot that needs to be improved.

● (1635)

Mr. Ryan Williams: We'll go to Mr. Hatfield online.

Mr. Matthew Hatfield: I'd rate it between a three and an undeciphered symbol. We simply don't know what AIDA will be in the final version. We don't have every piece of the puzzle.

As a starting point, as a white paper that we could then run a consultation around, sure, it's a great start. However, at the speed it's moving, I can't give it a positive rating.

Mr. Ryan Williams: Thank you. I think that follows the testimony that we've heard. It seems that this was just brought as an afterthought—with no public consultation.

I'm going to leave it at that. I think we can all agree on that.

Ms. Polsky, I do want to talk about privacy impact assessments. I know that you have an intimate knowledge of them. I'd like to ask if we should make them more widely used in our privacy regime.

Ms. Sharon Polsky: Should we make them more widely used? Yes, absolutely. The problem comes in when many organizations leave it to the operational people in the departments to do the preliminary assessment, such as on whether they think this new product or system or whatever will have an impact, when the people do not understand what privacy is, what privacy laws require and what the rights and responsibilities are.

They're under the gun. They have budgets. They have deadlines and go, “Nope, no privacy problem here.” They don't understand the unintended consequences. They don't understand the technology, the law or the business side of it. They're looking at it from a very narrow perspective. That's the first point. We need more education. There needs to be a mandate about all of this to the people in the organization.

The other part that's really critical is that an awful lot of organizations require that whoever does the privacy impact assessment follows the guidelines of their jurisdictional privacy regulator commissioner. Those tend to be checklists. They do not want fulsome legal analysis. They do not want the full picture. They want to be able to say, “We did a PIA. Tick that box. Move on. Next. Let's get business done.”

That's the public and the private sector.

Mr. Ryan Williams: The EU has legitimate interest assessments that have to be filled out by their privacy oversight bodies. Should we be using our PIAs to better define legitimate interests?

Ms. Sharon Polsky: We should, but we also need to have the people as the GDPR requires. The people who are in the position to do the PIAs, the privacy officers, must be independent within the organization and speak directly to the highest level of executive in that organization.

Now they are underlings. Even when they are lawyers who do the privacy work, a lot of our members who are the access and privacy people in the organization have to report to a very lengthy chain of command within the organization very often, and they don't have much say. They have very little authority. That has to be changed.

Mr. Ryan Williams: Thank you, Mr. Chair.

[*Translation*]

The Chair: Thank you very much.

Ms. Lapointe, you have the floor.

Ms. Viviane Lapointe (Sudbury, Lib.): Thank you, Mr. Chair.

[*English*]

Mr. Andrey, I would be interested in hearing your thoughts on Bill C-27 and its objectives to address online misinformation and online harm.

Mr. Sam Andrey: Sure. I would be delighted. We think a lot about misinformation and online harm. The government has been considering legislation on online safety for a while and been consulting about it. We're urging that it move forward.

We were surprised, but I think pleasantly surprised, that the AI act now would be a potential vehicle to address some of the harms of content recommendation systems, or “social media”, as most people refer to it. It was in Minister Champagne's list. If the online safety legislation doesn't move forward, or if it really focuses heavily on content like child sexual exploitation and terrorist content more specifically, then I think this could be a vehicle in which we attempt to regulate the recommendation systems and their algorithmic amplification for potential harm. I think it's a good example of the type of thing that will take time to do correctly through the regulatory process, but I think it is a potential way.

Specifically on the generative AI component of it, in the voluntary code that was referenced, there's a proposed requirement for what's called watermarking. It's basically people being able to detect that it's a manipulated image or video or a deepfake. Especially as generative AI improves and our ability to trust anything we're seeing with our eyes breaks down, that type of technical and regulatory response will be very important.

That's just an example of how we can use this bill. I think that is very important.

● (1640)

Ms. Viviane Lapointe: One of the challenges we have is in trying to strike that balance between freedom of expression and the need to combat online harm in this legislation. What are your thoughts on how that balance has been struck?

Mr. Sam Andrey: It's a really core challenge, especially when it comes to misinformation, as opposed to some other content that's more clearly illegal, say things like hate speech.

With respect to misinformation, yes, we have to be very careful, but I tend to focus on a "more speech" approach rather than a censorship approach, which is building the systems where fact checkers are adding context to things we're seeing online and where things like deepfakes are being labelled so people know it. It's not to say there won't be manipulated imagery online, of course—that has always been the case—but people should know that what they're seeing is that. I think that's a way to balance freedom of expression and the real harms that are happening with respect to disinformation.

There are other pieces about algorithmic propagation and the financial motives that we can get into, but I think, at its core, any legislation or regulation through the AI act that tries to regulate speech needs to put at the forefront. Companies need to consider the freedom of expression alongside the other aims.

Ms. Viviane Lapointe: You talked about the bill including provisions related to AI and automated content moderation. In your opinion, what's the role of AI in enforcing these regulations?

Mr. Sam Andrey: That's a good question.

Most large online platforms use automated systems to do content moderation. Those can produce imperfect results. Right now, you're seeing legitimate pro-Palestinian expression being caught up in filters about Hamas, just as an example. These systems are imperfect, though for the scale of the systems, they're often necessary.

We think, though, that a potential online safety bill, or potentially the AI act, could create additional recourse for users to challenge systems. The EU Digital Services Act, which is their equivalent, provides the ability for users to receive an explanation as to why it was taken down and to appeal it. That's something we don't have here in Canada, just as an example.

Those kinds of content moderation systems are getting better over time. AI and large language models will undoubtedly help make them more effective, but I think, at the end of the day, basically the recourse for a human to be in the loop for those things that are grey is absolutely necessary.

Ms. Viviane Lapointe: In your opinion, what are some of the biggest challenges that Canada may face in implementing and enforcing this legislation effectively?

Mr. Sam Andrey: The AI or just in general...?

● (1645)

Ms. Viviane Lapointe: It's just in general.

Mr. Sam Andrey: It will be a challenging task. I think part of the challenge is that AI—and it's the reason that the bill exists in the first place—is going to start to affect every part of the economy, and it's going to be used in a bunch of different sectors in a bunch of a different ways. The regulator, whoever it is, is going to be tasked with having to develop deep expertise in a lot of functions of the economy to be able to regulate its potential risks and harms. I think that is number one.

I think it's also why the existing regulatory model is so worrisome. It's so deeply embedded within the department. We would urge creating more independence. There's a bunch of ways that could happen. You could make it a parliamentary appointment that's by itself. There have been some suggestions of giving it to the Privacy Commissioner, which obviously has some resources in infrastructure and expertise. I can see both sides of that; the risks of AI are broader than privacy. At the very least, make it a GIC appointment, which is imperfect but at least creates some accountability and rules around the appointment. At the moment, it's not even that.

I could have more to say about that, but I'll leave it there.

Ms. Viviane Lapointe: Thank you.

The Chair: Thank you.

I'll give the chance to Mr. Hatfield to add his comments.

Mr. Matthew Hatfield: I have a quick observation on Canada's positioning here. A lot of the AI models and outputs of the AI models are going to be created in other countries but will still affect Canada. We can't prevent some of the worst harms that could occur from AI on our own. They're going to affect us even if we have incredible laws here.

However, Canada could distinguish itself by having uniquely poor AI rules. We could go it alone, in the sense of having some major misses on preventing harms and allowing people to do things in Canada that are not permitted elsewhere. That's why I'm very concerned about the balance of costs and benefits in our going it alone and trying to be out first. I'm not sure that we can win big. I do think that we can lose big.

The Chair: Thank you.

[*Translation*]

Mr. Savard-Tremblay, you have the floor.

Mr. Simon-Pierre Savard-Tremblay: Thank you, Mr. Speaker. I assume I have the floor for two and a half minutes.

Mr. Andrey, in your report last month, you state that Quebec has the highest rate of use of AI in Canada. You also say that only 2% of companies cite security or privacy concerns, and an even smaller percentage cite legal obstacles. On the other hand, you also point out that companies co not have all the information they need to fully understand the value and profitability of these technologies.

First of all, why is the rate of use of AI higher in Quebec than in other provinces?

[*English*]

Mr. Sam Andrey: That is a great question. I think Quebec has done a nice job of creating a robust AI ecosystem, and that shows up in the numbers and how more Quebec businesses have adopted AI systems. The number is still not that much higher than in the rest of the country. It's still in the single digits, but it's better than the rest of the country. We have lessons to learn there.

On AI adoption, I know that we're talking about privacy risks and harms, but for Canada's prosperity we have to become a more innovative and productive economy. Technology is a key enabler of that. I don't want to come across as anti-AI. It is very important, but we need to do it responsibly. For them to increase adoption, companies want assurance that what they're going to deploy is not going to get them in trouble, that it's going to be safe and that it is subject to legal guardrails. These things work together, and there's also work to be done on workforce development and talent and a whole bunch of other obviously enabling conditions. However, I actually do think that the AI act can help in assuring companies, especially small and medium-sized enterprises that are not going to have lawyers to access to think about these things, that the AI they're going to purchase is safe to use.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: You talked about it. You said that artificial intelligence should be used responsibly and that it is a good tool for prosperity.

What needs to be included in Bill C-27 so that we can promote the responsible adoption of AI?

[*English*]

Mr. Sam Andrey: I think I got that.

Do you mind repeating the question? I'm sorry.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: You said that AI must continue to be adopted responsibly, because it contributes to the prosperity of our people and our economies.

What needs to be incorporated into Bill C-27 to make that happen?

[*English*]

Mr. Sam Andrey: Thank you.

I think the ability for the law to meaningfully prevent and ban outright bias in these systems, psychological harm and misuse and malicious use depends on the context of the system we're talking about, but in financial services, in health care, in content moderation, which we were talking about, and in generative AI, there's a whole variety of ways in which harms and risks could manifest.

What is good about this bill is that it is comprehensive and wide in terms of its application, so the regulator, when it gets stood up, will have a big job in starting to prioritize which to focus on first. Minister Champagne's list provides some hints at that, but I think to secure responsible adoption, we need to focus on the systems that are also going to be used by a lot of businesses.

Generative AI is a good example of that, in that, increasingly, businesses are starting to think about how they could embed those in their processes to make their businesses more efficient.

● (1650)

The Chair: Thank you.

Mr. Masse, go ahead.

Mr. Brian Masse: Thank you, Mr. Chair.

Maybe I'll go to Mr. Hatfield first and then I'll go to the other panellists quickly as well.

What's your opinion—or do you have one—on an AI and data commissioner as an independent officer of Parliament? That could be done even before or without this bill, similar to the case with the Privacy Commissioner, the Competition Bureau and so forth. It seems as though there is almost consensus on the Hill that it's really going to involve almost all different parliamentary functions and committees and so forth.

That's for you, Mr. Hatfield, and then if anyone else on the panel in the room would like to comment, I have a couple of minutes, so please do so as quickly as you can.

Mr. Matthew Hatfield: Yes. I think that would be immensely valuable, especially getting them started on reporting to Parliament on what they think is going on. Evaluating the legislation, either before or after it's passed, would be valuable.

Mr. Brian Masse: Excellent. Thank you.

Is there anybody else on the panel...?

Ms. Sharon Polsky: Yes, if I may.

I think it's a terrific idea if the law requires that the regulator and others be fully funded so that they can actually do the job they are tasked with doing, and if they are able to write it into AIDA when it's split out from Bill C-27 and becomes its own, please, so that before AI products are allowed to be put on the market—I don't care from where in the world they are—they must go through basically a testing sandbox. It's not the self-interested vendor saying, “Don't worry your pretty little head; it's not biased.” It's an independent officer of Parliament whose office will identify and test the products—confidentially, with no secrets being divulged and no IP worries on behalf of the companies—so that, the same way any other product needs to be fit for purpose before it's released on the market, AI products must also.

Mr. Sam Andrey: May I just add quickly to that?

Let's not also make the same mistake we did with the Privacy Commissioner. If it's going to be set up as an independent agent, then it has information-sharing powers with the government and with other commissioners. A lot of these investigations are going to span competition, privacy and other functions.

Mr. Brian Masse: That's actually a good point, Mr. Andrey. With that, though, would you agree with its having more of a confidential quarter to it? At some point there has to be public accountability in terms of, especially when a decision is made, balancing out the private investment that's taking place with, too, full accountability to the public about how and when a decision was made and why.

Mr. Sam Andrey: Yes, absolutely. I think just information-sharing powers to enable that investigation...but yes, of course, when it comes to enforcement or a fine or a decision, it should be clear who is doing what

Mr. Brian Masse: Thank you, Mr. Chair.

Thank you to the witnesses.

The Chair: Thank you to all.

Just before I turn to Mr. Vis, I'd like to seek unanimous consent from committee members. As you all know, we received a Standing Order 106(4) to study the SDTC affair. Based on the timeline, we would need to study it on Monday. I am asking for unanimous consent to do it on Tuesday. We have a committee meeting on Tuesday, but so far the invited witnesses have declined, so that would be a good use of committee time.

If all are in agreement, we would do it on Tuesday. Do I have unanimous consent?

Some hon. members: Agreed.

The Chair: Thank you so much.

Mr. Vis, the floor is yours.

Mr. Brad Vis (Mission—Matsqui—Fraser Canyon, CPC): Thank you, Mr. Chair.

Mr. Hatfield, last year OpenMedia gave Bill C-27 a failing grade of D. Referring specifically to protections for children, how would you grade the protection of children in Bill C-27?

● (1655)

Mr. Matthew Hatfield: I think it's good to have some unique protections and to force companies to handle them slightly differently. I do think we need to ask ourselves whether many of the protections enjoyed by children shouldn't be enjoyed by everyone in Canada. It's sometimes not clear why only children deserve certain standards of protection.

Really, giving ongoing informed consent, and withdrawable consent, to everyone would be valuable.

Mr. Brad Vis: Okay.

Bill C-27 does not include a definition of “sensitive information”, yet it does outline that children's data would be subject to sensitive information. Do you think it's problematic that the government did not include a definition of sensitive information for both general purposes and specifically for children?

Mr. Matthew Hatfield: Yes, absolutely. At the very least, have an indication of how that would be determined by regulation.

Mr. Brad Vis: Do you think it's ethically wrong if the government enables companies to have the ability to monetize biometric and data locations of children and to sell that information for a profit?

Mr. Matthew Hatfield: Yes, I do, but I also think it's ethically wrong for adults. I think we should both be protected from that.

Mr. Brad Vis: Okay.

Would OpenMedia support amendments that would specifically address protecting biometric information for children and their location information?

Mr. Matthew Hatfield: Yes, depending upon the wording. Our feedback might end up being that we should extend this to everyone, with a small extra portion of privacy for children.

Mr. Brad Vis: Thank you.

Ms. Polsky, what in your mind are some of the biggest gaps in Bill C-27's protection of children, beyond the sensitive information that I have already raised?

Ms. Sharon Polsky: On privacy legislation, we all have a right to privacy without an age limit, but when it comes to children, we already have children's information being gathered surreptitiously and shared with the data broker industry without consent—of their own or their parents'.

Mr. Brad Vis: Do you believe that's ethically wrong?

Ms. Sharon Polsky: Of course it's ethically wrong. It's reprehensible. It doesn't give parents, guardians or the kids any say. Then they get bombarded with all sorts of...whether it's online ads, bots or negative commentary. We know now that—

Mr. Brad Vis: Would it be morally wrong?

I'm the parent of three children. I'm in a unique position to do something significant for kids. Would it be morally wrong for me as a legislator if I didn't take severe action or put forward major amendments to this bill to ensure that companies couldn't commercialize the data of children?

Ms. Sharon Polsky: I think you would be failing as a parent. I also have children. I think it's incumbent on all of us, whether we have children or not, to protect the kids. Whatever goes online now, they get to live with for the rest of their lives, and it gets monitored. Yes, it would be an abdication of parental responsibility.

Mr. Brad Vis: In respect to sensitive information—I'm sorry to cut you off—do you believe it is incumbent to provide not only a fulsome definition of sensitive information but also specific examples so that we do not leave it to regulators or judges to determine what sensitive information is regarding children?

Ms. Sharon Polsky: It's going to be a monumental task to do it, yes. I've never encountered anything where it's been possible to create an exhaustive list—conceptual and categories perhaps. It has to be able to be expanded and reviewed—expanded is necessary—frequently.

Mr. Brad Vis: What about in this approach? Some of my colleagues have mentioned proposed section 18 of this legislation. I believe the last paragraph in proposed section 18 outlines "any other prescribed activity." What if I used the language like "any other prescribed activity", but in respect to limiting companies from using the information of children? It would be a broad section that would provide protection for children so as to avoid any commercialization of data for children that is unnecessary.

Ms. Sharon Polsky: As an idea, sure, but then how do you operationalize and police it? How do you make sure the companies are actually complying with the legislation?

They've done a poor job of complying with 20-year-old privacy laws. What's going to make this any different or any better?

● (1700)

Mr. Brad Vis: Then what do we do to enforce these rules to protect our kids?

Ms. Sharon Polsky: It might be easier to say what we don't do. We don't leave it to people who don't correctly understand what privacy is and what the technology is, does and can do. We require a broad consultation of the people who really do understand it at a deep level. That, I think, is not the technology companies that are self-interested.

I'm all for companies making profit and shareholders, investors and domestic economic advantages—sure—but our privacy is not their concern, and they've done a poor job until now.

Mr. Brad Vis: I'm thinking ahead 15 or 20 years to when there's going to be other privacy legislation in Parliament. In the meantime, with technologies changing so quickly, is there any other alternative other than doing something pretty fundamental here to put forward a bill that goes to the nth degree to make sure that children are protected in every single circumstance—

Ms. Sharon Polsky: Yes, turn it around.

Mr. Brad Vis: —and that their data cannot be used under Canadian law?

Ms. Sharon Polsky: Turn it around, so that it's no longer up to the companies. Make it so that—thee and me—we have the authority to grant permission to the companies.

When we look at that, I caution that, when it comes to companies or legislation, it will require age verification. We already have companies saying that in order to make sure that the children aren't looking at this content, provide photo ID—government-issued photo ID of mom, dad and the kids.

All they're doing is collecting that information. Why should we trust that they're going to protect that any better than the information they already don't protect well? It's so complex. That's why, please, involve our organization, my colleagues' organizations and the people who actually understand this from an operational level.

Mr. Brad Vis: Jim Balsillie said in our meeting that, in a previous time, kids could go back to their room at the end of a hard day at school and lick their wounds.

Can we get back to that in Canada where kids truly have freedom from technology once again? Can we as legislators help them get there?

Ms. Sharon Polsky: I'm very pleased to see recently kids in my neighbourhood, seven-, eight- or 10-year-olds, walking without a parent at arm's length, without an adult. From some psychology experts in the States, there was a report recently that children have suffered because they have not been allowed to play outside. Go climb a tree. Go fall. You won't do it again. They learn their limits. We need that.

That is I think a public policy decision from governments across the country at every level. It's not just a matter of teaching kids in school digital citizenship, feeding them and handing them digital devices. Take the digital devices away and make the kids think again. Tell them to go and play. Run and play and be kids. Don't make digital everything the be all and end all, as if you're going to be the odd man out if you don't use these technologies. Let them be kids. Do you know what? Go back to pen and paper. It's a whole lot more private. Old fashioned is—

Mr. Brad Vis: Thank you for your time.

The Chair: Thank you very much.

Mr. Hatfield, I'll give you the last comment for this round.

Mr. Matthew Hatfield: Can I just suggest the best way to protect the data of young people is to provide a very high level of data protection as an option to everyone?

If someone indicates that they are a minor when they sign up, default everything to the highest level of protection and don't change that until they're not a minor.

The Chair: Thank you.

Mr. Gaheer.

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): Thank you, Chair.

Thank you to all the witnesses for making time for this committee. My first questions are to Mr. Lawford.

I was listening to your opening testimony. I was just a little bit thrown off by it.

I'll just ask one question because I do have questions for the other witnesses as well.

You had mentioned something about business activities, that the exception is there. Information can be used without the knowledge or consent of the individual if the information is used for a business purpose. You said this information could be used against individuals. Is that correct, from your opening testimony?

● (1705)

Mr. John Lawford: Yes. This is where you get into disputes with businesses about whether what they are collecting is necessary for the purchase. If you go into Tim Hortons and you want to order your coffee when you're waiting in line, so when you get to the window it's ready, do they need to track me all across town afterwards because that's the default in the software?

It's that kind of thing. There's a difference in opinion from Tim Hortons to me about whether that's necessary.

Mr. Iqwinder Gaheer: I'm sorry to interrupt.

I'm looking at the actual legislation itself, the bill. There are clear safeguards. It says that the information can be collected without their knowledge and consent if it's used for the purpose of a business activity, but proposed paragraph 18(1)(a) says that there are conditions. One is that "a reasonable person would expect the collection or use"—of that information—"for such an activity". More importantly is proposed paragraph (b), that "the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions."

It's very clear there's a safeguard in the bill itself that the information that's collected can't be used against that individual.

Mr. John Lawford: Right.

I think the business answer would be that we're not going to use that personal information to disadvantage you. We're going to offer you benefits. There's a new pumpkin spice latte. We're going to give you a coupon while you're waiting in line. Some people might accept that. Other people might think that's creepy. The trouble is that the first standard you mentioned in 18(1) is an objective standard. If it bothers me personally, I don't have the choice to say, "No, that bugs me personally. I don't want your coupons." Right now, under PIPEDA the decision is more subjective and it's personal to me. I just don't give you my consent.

This flips it around backwards is what I was trying to say.

Mr. Iqwinder Gaheer: What's the alternative then?

Would you just remove this clause altogether?

Mr. John Lawford: Section 18 is gone, yes.

Mr. Iqwinder Gaheer: What about the fact of stifling innovation, stifling business, and that fine line you have to walk?

Mr. John Lawford: I don't buy that, because businesses are functioning very well right now. I don't know of any innovation that's being stifled by the present law. Perhaps the Business Council said something different the other day.

If you take proposed section 18 out.... Now consider that proposed section 18 wasn't in Bill C-11. Apparently the department didn't need all these exceptions in the first version. Now, it's in. I'm just saying to take it out because businesses can function at the present time. I think to remove the general right of subjective consent from all Canadians is a pretty big lift. I want to see a lot of innovation being stifled before that gets taken away.

Mr. Iqwinder Gaheer: This bill has gone through so much consultation over four years across companies, civil society and academics as well. We are radically improving enforcement powers, and we're increasing the requirements on businesses.

My other question is for Mr. Konikoff.

Regarding the tribunal, we heard from Michael Geist that the tribunal could accelerate and improve access to justice if it was "properly constituted". It's mandated that it requires at least three experts in privacy law, and it could offer more specialized and faster resolution than our traditional court system. As a lawyer, that means a lot to me.

In your opening brief, you said you wanted to remove the power of the minister to recommend tribunal members. Does that mean you will support the tribunal?

How would you want the tribunal to be constituted?

Mr. Daniel Konikoff: I think the question of whether I support the tribunal is contested.

It seems as though it has a fundamental problem with that independence component. The capacity for the minister to appoint what would essentially amount to, as I wrote here, part bureaucrat and not independent judges or officers at arms length of Parliament, would pose a tremendous challenge to any sort of claim that can be made of the tribunal's independence, should it exist.

Mr. Iqwinder Gaheer: I'm cognizant of the time.

How would you do it differently then?

Mr. Daniel Konikoff: It's on me to point out these concerns. It's not necessarily on me to entirely reconstitute a legislative body.

Thank you.

Mr. Iqwinder Gaheer: Thank you.

[*Translation*]

The Chair: Thank you very much.

Mr. Généreux, you have the floor.

Mr. Bernard Généreux (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, CPC): Thank you, Mr. Chair.

I want to apologize. I had to go give a speech in the House, so I may have missed some things. I'd like to avoid repeating anything that may have already been asked in my absence. That said, Mr. Lawford and Ms. Sai, I'd like to ask you some questions to follow up on Mr. Gaheer's question about the tribunal that the bill aims to create.

I have great respect for Mr. Balsillie, whom the committee received on Tuesday, and for Mr. Geist, who appeared last week. I digress to say that, so far, no one has spoken positively about this bill. I think we have a serious problem.

Moreover, Mr. Lawford and Ms. Sai, you're saying that we should remove the provisions to create a tribunal from the bill because that could slow down the process should any lawsuits be filed after the bill comes into force.

Could you elaborate on that?

● (1710)

Mr. John Lawford: I will answer first and Ms. Sai can round out my answer.

Under the current regime, a decision is made directly by the Privacy Commissioner of Canada. The process takes about a year, in the case of major investigations.

Based solely on the experience of the Competition Tribunal, I estimate that this added step will extend the process by a year to a year and a half. In addition, it will benefit companies that appeal against a Commissioner's decision. I see no benefit to consumers, who are typically the ones who benefit from the Commissioner's decisions.

Mr. Bernard Généreux: Earlier, Ms. Sai, you made a comparison with rocket fuel, but I forgot the rest of the sentence. It was something about pouring gasoline on the fire. I don't remember exactly what you were referring to, but I think it was clause 39 as proposed in the bill.

[*English*]

Mrs. Yuka Sai: Are you referring to proposed section 39, which is the “Socially beneficial purposes”?

Mr. Bernard Généreux: Yes.

Mrs. Yuka Sai: When I refer to proposed section 39, what it really serves to do is degrade public transparency and and public trust in our public institutions because of two things.

First, it requires businesses to de-identify personal information before transfer to a public institution. That means they don't have to adhere to knowledge or consent requirements as long as they de-identify. The other thing proposed section 39 does is allow the minister to prescribe additional public entities and new socially beneficial purposes with which to engage this exception to knowledge or consent. This facilitates unwarranted secrecy in the way that public institutions obtain personal information from the private sector to use in the policy decisions that affect us all.

[*Translation*]

Mr. Bernard Généreux: Thank you very much.

I'd now like to address Mr. Hatfield of OpenMedia.

At the beginning of your presentation, you said that AI is going to have an even greater impact on people's lives than the advent of the Internet some 30 years ago. What exactly did you mean by that?

[*English*]

Mr. Matthew Hatfield: We're in a funny space where no one is quite sure exactly how generative AI is going to play out. There are huge disagreements around that. When I shared that view, that was the view of about a third of our community, who said the impact was going to be comparable to or bigger than the Internet.

About 80% of our community thought it would be bigger than smart phones. As I represent OpenMedia, I'm somewhere in between bigger than smart phones and the size of the Internet. That could be untrue, but I think we need to prepare for a range of possibilities, which could include, frankly, generative AI largely replacing the Internet as we know it and most information coming through working up some kind of AI that speaks to us in the language we speak.

[*Translation*]

The Chair: Thank you very much.

Mr. Sorbara, you have the floor.

[*English*]

Mr. Francesco Sorbara (Vaughan—Woodbridge, Lib.): Thank you, Chair.

Welcome, witnesses.

I apologize for not being here at the beginning of the committee meeting. Nonetheless, I do have a few questions.

I can start off with Sam from TMU. You have a view, I would say, in terms of the artificial intelligence and data act, in terms of what amendments you could or would probably propose. Also, perhaps you can comment, please, on your view of the act in general.

Mr. Sam Andrey: Sure. I think the bill needs lots of amendments and improvements. I think some have been tabled by the minister already, and several are noteworthy improvements from the current version.

Maybe I'll just focus some comments on things I haven't yet raised.

I think the current model is really focused a lot on audits that organizations will potentially do themselves to determine the risks and harms. AI auditing is not yet a codified practice. It's not even really clear what field of expertise should be doing these audits. Is it computer scientists? Is it accountants? Is it lawyers? This is going to take time to develop, and it has to be accompanied by robust standards.

As that happens, the bill as it stands doesn't have a complaint mechanism. It's silent on how the minister will establish grounds to believe an investigation is required. There are no whistle-blower protections for people who bring things forward. There's no ability to do pre-emptive audits. I think my biggest challenge with the act is in its regulatory model, and I do think that those pieces can be fixed.

● (1715)

Mr. Francesco Sorbara: Thank you.

I'll go over to the Privacy and Access Council of Canada. As this committee meeting is going on today, in Europe there has been a large AI meeting. All the leaders were there—the U.K. leader, the Italian leader and so forth.

I want to ask your thoughts in terms of the artificial intelligence act. I think there was a document dated April 14, 2023, with regard to the EU becoming likely the de facto global standard for general-purpose generative AI intelligence systems. I may be very humble about this, but with the speed at which AI and other forms of new technologies are taking place, I don't know how many people actually understand them.

We were over in Europe several months ago as chairs of the Canada-Europe Parliamentary Association. We had some folks actually from Montreal there, who gave us presentations.

It's very complicated and so forth, but I would like to hear your thoughts in terms of the EU's proposed AI act and where that will take not only the EU but the world, because it seems there is some "first mover" going on, if I can use that term.

Ms. Sharon Polsky: I think each country wants to be the first. As was questioned earlier, is that the right choice? Canada is marching forward and pushing this through, but to what benefit and, more concerning, to what harm?

When it comes to the EU and the U.K., yes, they've given thought and lots of consultation, but I think it's important to not consider these pieces of legislation in isolation, because on one hand we have robust AI regulations coming out of the same country that just passed the euphemistically named "Online Safety Act" that requires all content to be monitored, including yours, because the Internet is global.

How do we protect anything when AI is behind the scenes? AI is used in these buildings, in airports and in shopping centres. It's everywhere already.

Yes, they have a jump on Canada. Is it the right direction? It's certainly better than what we have in Bill C-27. There is no disagreement on that, whether from today's meetings or from many of your previous witnesses. We can look to our European counterparts. They are on a better path. That's about as generous as I can get right now.

Mr. Francesco Sorbara: Thank you.

That's it for me, Chair.

The Chair: Thank you very much.

[*Translation*]

Mr. Savard-Tremblay, you have the floor.

Mr. Simon-Pierre Savard-Tremblay: Thank you, Mr. Chair.

My next question is for Mr. Lawford.

During certain testimonies and meetings with people in the industry, we heard a great deal of unease about the lack of detail in part 3 of Bill C-27. I Am talking about the part that enacts the Artificial Intelligence and Data Act, as well as the criminal liability it imposes on companies using high-impact AI systems.

To what extent do you think all this will need to be clarified, if we are to promote greater trust and ease among businesses, and SMEs in particular, while maintaining rigorous protection provisions? Where is the balance?

● (1720)

Mr. John Lawford: I have a problem with the fact that the bill distinguishes between large companies and small and medium-sized companies, because, in the case of the most intrusive systems, I doubt that the size of the company matters. Let's say someone opens a new gym equipped with several tracking capabilities, for example. Whether it's a very small, very innovative company or a large one like GoodLife Fitness, what difference would it make to the individual whose data is being collected in order to establish their profile and locate them?

I believe that the Privacy Commissioner is the best person to assess the need to set a higher fine for certain companies, and I'm certain that the appropriate amount will be chosen for each particular case. In addition, the court will be able to determine whether this is too great a burden for small and medium-sized businesses.

I don't know if I've answered your question.

Mr. Simon-Pierre Savard-Tremblay: In 30 seconds, I won't have time to formulate another one, so thank you.

Mr. John Lawford: All right, thank you.

The Chair: Thank you very much, Mr. Savard-Tremblay.

It would normally be Mr. Masse's turn, but he had to leave a little early. He agreed to give me his time. So, I'm going to take this opportunity to ask you a few questions, too.

[*English*]

I'll just echo some of the concerns my colleague Mr. Van Bynen has raised about consent fatigue and also what Mr. Perkins talked about when it comes to the Zoom contract, where the terms can be changed at the discretion of the organization.

In my mind, consent, when it comes to online activities, is a bit overrated, because there is such a big imbalance in power between the user and the organization. We cannot say that there is a meeting of the minds when privacy lawyers don't even bother to read the terms. I'm a lawyer. I haven't practised in a while, but I don't read the terms, and we need to use these apps in our day-to-day lives.

This is what, to me, the role of the legislator is: to strike that balance for consumers, kind of like in a landlord and tenant situation, where the terms are very clearly defined. I gather from your interventions that this balance has not been struck in this bill. What would be absolutely essential for us to strike that balance?

Go ahead, Mr. Hatfield.

Mr. Matthew Hatfield: I'm glad you came back to consent fatigue, because many of us feel consent fatigue much of the time, but not always. This is where ongoing consent is very important. It's having the power to have a simple, easy-to-understand dashboard that essentially has a privacy slider from here to there, and either I can come in before I start using the service and say, "I want to be here" or—and this is crucial—I can come back after having used the service for a period of time and say, "I have changed my mind. I had consent fatigue when I first signed up. I ended up clicking through something I shouldn't have, but now I have thought about it, I have the presence of mind and I no longer want to be on the most permissive side of this."

The ability to revoke my consent or at least restrict the way my data is being used in a way that, to date, I haven't been able to is very important as well.

The Chair: Are there any other comments?

Go ahead, Mr. Konikoff.

Mr. Daniel Konikoff: Thank you. I have a quick comment in this regard.

On the subject of consent fatigue, perhaps that's something that private industry could look to try to combat by coming up with innovative ways to develop more enticing or readable materials that are more informed. I believe that would allow for people to give more informed, more meaningful consent.

I could point to the work of some scholars out of York University, such as Jonathan Obar. He is working on a project to make consent and privacy policies more user-friendly, so he's putting them in terms that users may understand. If it's an app that is predominantly used by teenagers who look at memes, it's folding the language of memes into user consent. Putting consent in the language of the user is one way around that.

● (1725)

Ms. Sharon Polsky: If I can, I'll add to that. Right now, we already have a problem, because some people say there is consent fatigue, but before you even see the website you've called up, the fact that you have called up that website has been communicated to Facebook through Meta Pixel and hidden devices that you don't have the opportunity to consent to or withhold consent from. It's going on in the background. Even if, as Matt suggested, you get the opportunity to withdraw your consent, that doesn't flow to all of the dozens and hundreds of organizations in the data brokerage industry that are bidding on and exchanging your information. You don't have a direct relationship with them. You have no control.

I think the law needs to put very clear prohibitions on industry to say you're allowed to do certain things, and here is a list of the types—not specific actions—of things thou shalt not do, including dark patterns—where the consent is, "No, I don't consent" and it returns "Are you really sure? Do you want to reconsider this?"—or the colours used. A lot of study has been done about this sort of thing. It's manipulative. Whether it's for adults or children, regardless of intelligence, education or competence, it is manipulative. It needs to be banned in Canada as well.

The Chair: Go ahead, Ms. Sai.

Mrs. Yuka Sai: First, I'd like to touch upon this idea of whether we are balancing business interests with the privacy interests of individuals. I think we have to remember that businesses, especially digital platforms, already exert an incredible amount of power and leverage over individual consumers. Already, there is no equal balancing there.

What we would like to see in this bill is a prioritization of consumer knowledge and consent, rather than a bill that seems to treat consumer consent as an inconvenience for businesses.

On the topic of consent fatigue, that's a concept we take umbrage with because it seems to be used by industry to push for a progressive paring down of consent. The question that seems to be asked right now is what types of business activities no longer need to be consented to because consumers are tired of the lengthy, repetitive consent requests. The question we should be asking is how we overcome consent fatigue by innovating how consumers can manage their preferences in an easy-to-understand and accessible way. Basically, it's retaining the same level of control over consent as before, but in new ways.

This term "consent fatigue" really shouldn't be the basis for getting rid of consent based on ever-changing consumer expectations that are, in truth, being shaped by the industry itself.

The Chair: Thank you very much.

Go ahead quickly, Mr. Andrey, because I have one last question.

Mr. Sam Andrey: Sure. I'll be quick.

In terms of consent fatigue, there are new exceptions and existing exceptions where people don't even need to be provided knowledge of the things that are happening. For workers, say, no knowledge or gathering of consent is required.

A different committee is at the moment studying the risk of TikTok potentially sending our personal information to China. There are no limits in this bill on any Canadian company sending data to China.

Those are the types of protections that the bill could put in place in terms of comparable protection, so that you don't need to read TikTok's long privacy policy to find that it's in there. I think it's not just about consent. It's also about the protections that are there by default.

The Chair: Thank you very much.

I have one last quick question.

Mr. McSorley, you mentioned proposed sections 47 and 48 concerning national security, and proposed section 47 in particular. Can you repeat how it differs from PIPEDA? In PIPEDA, under paragraph 7(3)(d), an organization that suspects that an activity is a threat to national defence can still disclose that information.

Can you repeat what difference there is?

● (1730)

Mr. Tim McSorley: I didn't raise the difference, because in fact it is the same. We simply believe that it shouldn't be continued under this new bill. We raised those concerns in the review, in the consultation around PIPEDA earlier, that this was already a problematic exception. We don't believe.... It's something that this committee could fix in moving forward with Bill C-27.

The Chair: That's very interesting. Thank you very much.

[*Translation*]

Thank you, everyone. That concludes today's meeting.

I'd like to thank the witnesses. It was very interesting

I'd also like to thank the interpreters, the support staff and the Committee clerk.

I hope everyone has a good evening. The meeting is adjourned.