HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

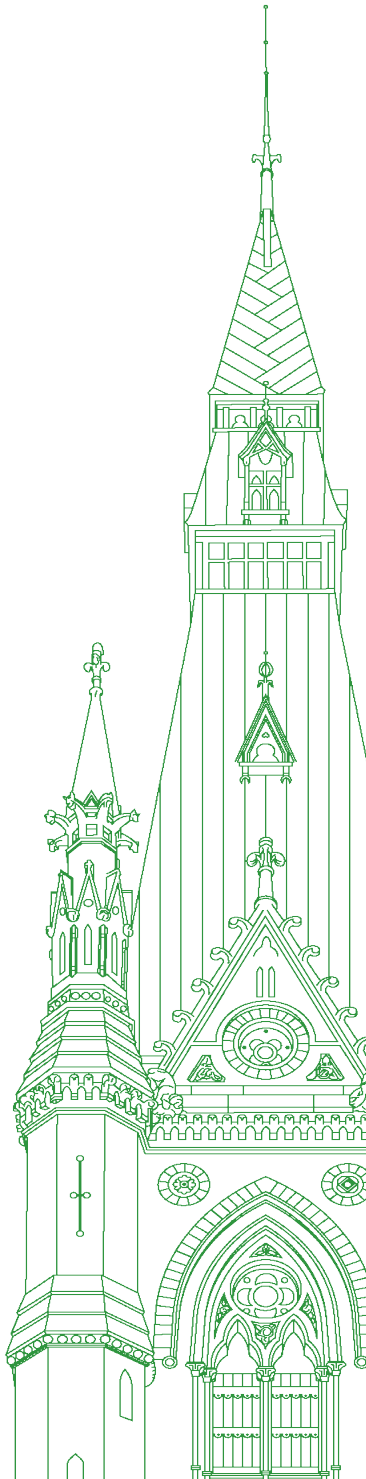
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 095

Monday, December 4, 2023



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Monday, December 4, 2023

● (1535)

[*English*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): I'm going to call this meeting to order.

I want to welcome everyone to meeting number 95 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Tuesday, January 31, 2023, the committee is resuming its study of the use of social media platforms for data harvesting and unethical or illicit sharing of personal information with foreign entities.

[*Translation*]

Today's meeting is taking place in a hybrid format, pursuant to the Standing Orders of the House. Members are participating in person, in the room, and virtually using the Zoom application.

[*English*]

I would like to remind all members not to put their earpieces near the microphones, because it could cause injury to our interpreters.

I would now like to welcome our witnesses for the first hour. As individuals, we have Brett Caraway, associate professor of media economics, University of Toronto; and Emily Laidlaw, associate professor and Canada research chair in cybersecurity law, University of Calgary.

Before we begin, the bells are ringing. I received unanimous consent from the committee to begin this meeting for the opening statements in advance of the votes. I appreciate the indulgence of committee members for allowing that to happen, so that we can listen to our witnesses.

Mr. Caraway, you have five minutes, followed by Ms. Laidlaw.

Mr. Brett Caraway (Associate Professor of Media Economics, University of Toronto, As an Individual): I would like to thank the members of the committee for the opportunity to speak today.

I'm an associate professor of media economics at the University of Toronto. I appear here today in a personal capacity, so the views expressed are mine and mine alone.

I want to speak about the risks posed by the underlying incentive structure of social media platforms. In doing so, I hope to convey some sense of the changes that have transpired in our media landscape and why there are, too often, divergences between public and private interests.

Digital platforms are major features of the information economy because of their capacity to reduce market frictions and lower transaction costs. To understand what I'm talking about, imagine how a social media app like Instagram might make a particular group of users, such as amateur photographers or travel enthusiasts, accessible to advertisers who want to target them with commercial messages.

In this scenario, there are actually three market actors. There are the users, the advertisers and the platform operator, and they each have their own set of incentives. Instagram has a financial incentive to maximize the number of users and their level of engagement. This makes the platform more attractive to advertisers. Advertisers want as much information as possible about the platform's users so they can minimize uncertainty, and users just want to enjoy the functionality of the platform with as little disruption as possible.

Multisided markets like these are nothing new. They've been a feature of mass communication systems since the earliest newsletters began selling advertisements in the 1600s. However, terms like “niche marketing” and “targeted advertising” only begin to scratch the surface of what actually transpires every time you enter a search query on Google, watch a video on TikTok, like someone's post on Facebook or retweet something. Information is gathered, auctions take place and commercial messages are delivered.

My concerns are not driven primarily by escalating geopolitical tensions or foreign threat actors, though foreign interference, misinformation, disinformation and radicalization are all genuine concerns. My concern is that these platforms, even when functioning exactly as intended, have adverse impacts on the public sphere. My concern is that the economics of platforms all but guarantees the propagation of disinformation, efforts to influence behaviour and the erosion of individual privacy.

My concern is born out of the realization that, in the economics of platforms, there is no effective upper limit to the exploitation of human attention. “Attention” might refer to the ability to concentrate on something, but from the perspective of society, it speaks to our collective ability to recognize problems and opportunities, to the horizon of our imagination and creativity, and to our ability to rise to the occasion to meet the world's most pressing problems. Attention is a renewable resource, but it isn't like any other resource. You can't hoard it like a precious metal. You can only direct it at something. In fact, that's the economic function of advertising: the allocation of scarce attention among its competing uses. How we choose to allocate our attention is important, both for individuals and for society. Our attention shapes who we are, who we might be and where we might go.

Economists often speak of “the tragedy of the commons”. The origin of the concept is problematic. As a metaphor, however, it can be quite useful. It alerts us to the propensity for overuse and exploitation of finite resources when we allow unfettered access to them. Digital platforms don't merely attempt to measure attention. They seek to modify it—to make it conform to commercial imperatives. Today's attention economy looks less like AMC's *Mad Men* and more like the speed-of-light trading that takes place in financial markets. The fundamental economics of this system is inconsistent with robust privacy protections.

The overriding economic imperative is to maximize data collection. It's not just the PRC or Russia. It's U.S. firms like Alphabet, Meta, Amazon and a host of data brokers you have never even heard of. As a consequence, our attention is exhausted. Its quality is diminished.

We have protections to safeguard other resources, such as water, air and habitat. We must likewise manage this renewable resource in a similar manner, in a sustainable manner, as we would air, habitat and water.

We are at an inflection point in Canada. It's my hope that we can take concrete steps to empower Canadians by creating a comprehensive regulatory framework for all digital platforms.

Thank you.

● (1540)

The Chair: Thank you, Mr. Caraway.

Ms. Laidlaw, you have five minutes to address the committee. Go ahead, please.

Dr. Emily Laidlaw (Associate Professor and Canada Research Chair in Cybersecurity Law, University of Calgary, As an Individual): Thank you, Mr. Chair, for the invitation to address this committee.

I am honoured to speak to you from Calgary and the traditional territory of the people of the Treaty 7 region and the Métis Nation of Alberta.

I've had the opportunity to listen to some of the witnesses and the discussion leading up to my appearance. With my time, I would like to pull us back to look at the broader legal issues at play.

My key message is that this is not just about privacy. Privacy is one piece of the pie. For example, Discord does not use tools to detect child sexual abuse content, and it does not monitor or offer a tool for reporting livestreamed content. That's a recipe for disaster. This is a safety design problem, not only a privacy one.

This is about platform regulation. The health of our information ecosystem depends on privately owned platforms and the choices they make in the design of their products, corporate governance, culture and content moderation systems. In short, platforms have tremendous power.

Canada is currently a laggard in regulating platforms. Much of what this committee has discussed would be addressed by online harms legislation, which we do not yet have in Canada. Europe, the U.K. and Australia all have laws to address these issues. In some cases, they are on their second-generation or third-generation law. Canada has zero federal laws that apply generally to platform regulation. We can learn from the good and the bad of these other laws, but it is time to act now.

What do we need, and what are the areas we must be careful about?

First, platform regulation is a field like protecting the environment, and multiple areas of law must work in concert to protect our safety and rights. In particular, privacy law and online harms legislation are mutually reinforcing, so we need both. For example, algorithms that push harmful content do so by harvesting personally identifiable information, which is covered by privacy law. However, the algorithm can also draw from anonymized aggregate data, which falls outside of privacy law.

Online harms legislation can better target the choices that platforms make about their product designs and content moderation systems. Social media mines data to determine likes and interests, but it is what it does with this that online harms laws can address—such as Meta amplifying emotive and toxic content on Facebook by treating angry and love reactions as five times more valuable than likes. This fuelled the spread of misinformation and disinformation.

Second, platforms are part of the solution. They can be important collaborators and innovators in solving problems. There is, however, a friction when they are almost state-like in their role. Some have their own national security teams, essentially setting national security policy.

We also depend on platforms to go above and beyond the law in addressing hateful content, disinformation and violent extremism, all of which are not necessarily illegal. However, that is not a substitute for law to set industry standards. Standards are needed. The examples I gave were platforms with relatively sophisticated governance structures. There are many popular platforms that minimally govern the risks of their products.

Third, when we talk about the risks of harm, we should be clear that not all risks are the same. Child protection, hate and terrorist propaganda, disinformation, and violence all have different dynamics and should not be distilled to one legal rule, except for the basic idea of corporate due diligence.

Further, when we talk about the risks of harm, these include risks to fundamental rights: the rights to freedom of expression, to privacy and to equality. Any analysis of solutions in law or governance must be through the lens of protection and promotion of rights. This is particularly challenging when it comes to addressing misinformation and disinformation because, except in narrow circumstances, it is lawful to believe and share false information.

I will leave you with this: What are the basic components needed in online harms legislation?

Platforms should have a duty to manage the risks of harm of their products and a duty to protect fundamental rights. There should be transparency obligations matched with a way to vet transparency through audits and access to data by vetted researchers. There should be the creation of a regulator to investigate companies and educate the public, and there should be access to recourse for victims, because this is a collective harm but also an individual one.

Thank you, and I welcome questions.

● (1545)

The Chair: Thank you, Ms. Laidlaw.

We are going to ask you to be patient because we have roughly 11 minutes left before the vote. That should take another 10 minutes or so, so we should be back in 25 minutes with our first round of questioning, if that's okay—if you can hang on.

I am going to suspend the meeting for the vote. We'll be back right after.

Thank you.

● (1545)

_____(Pause)_____

● (1610)

The Chair: I'm going to call the meeting back to order. I do note that there is closure, and a vote is imminent. We have roughly 45-50 minutes here. We've had the opening statements from the witnesses, and we appreciate their patience.

We're going to start our first round of six-minute questioning with Mr. Kurek.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Chair, and thank you to our witnesses.

I appreciate, as well, that in your statements you provided a number of practical suggestions. As always, feel free to follow up if there's anything additional.

Mr. Caraway, I found some of your work very interesting, because the economics of social media is certainly a fascinating subject. It's that balance between a service that is perceived to be free versus the cost associated with something that is quite expensive to run, like a social media platform. When talking about regulations and managing that, how does that get balanced, the consumer's desire not to have to pay for a service versus the demands associated with running a massive web operation?

● (1615)

Mr. Brett Caraway: That's a great question.

The thing I always tell my students is that there's no such thing as a free lunch. Even though it appears that you're getting these services for free, if it's an advertising-supported model of some kind, you're paying for that when you purchase goods or services later on.

Most of the platforms we're talking about in the social media realm run as multisided marketplaces. It is quite difficult to keep everybody happy. As I alluded to, you're trying to keep the advertisers happy, but the advertisers want as much information as possible about the users. The users just want to be left alone to use the platform, but they also don't necessarily want to pay for it. That's never a popular thing, except maybe in some online streaming contexts when you're looking at services like Spotify or Netflix. However, even in the subscription-based models, a company like Netflix, which isn't necessarily doing the same sort of data harvesting that companies like Meta or Alphabet are doing, is also gathering data on how the users use the platform and deploying AI for recommendation systems, etc.

There's always an economic imperative for the advertisers to demand more data; therefore, the platform operators will harvest more data. I think that speaks to the need for the government to step in and say, “Well, here are the enumerated rights that we consider, such as privacy for citizens.” I don't just mean including it in a preamble, but actually putting those in legal tests, so—

Mr. Damien Kurek: I apologize, but we only have very limited time here.

I would like you to follow up—in about 30 seconds, because I would like to ask some more questions—on the specific context of making sure kids are protected. Could you maybe expand a bit on how that plays into making sure that kids are protected from online harms, and what that looks like in the context of young people?

Mr. Brett Caraway: That's supposed to be part of Bill C-27, the formulations of some sort of protections for minors. If you listen to representatives from TikTok, they will tell you that they have self-regulation and that they are the vanguard of that. They would say that people 18 and under can't livestream, or the privacy settings are by default for people 16 and under, or people 16 and under are limited to 60 minutes. However, these are settings that can just be changed.

It is important for the government to step in and help parents out, because they are literally overwhelmed by all the different social media platforms, and, of course, teens are on these platforms, depending on whom you ask, four to five hours a day.

Mr. Damien Kurek: Thank you very much for that. I would just emphasize that "to help parents out" is a great line there.

Ms. Laidlaw, we're talking about protecting young people. There's a range of harms on social media, from things like bullying all the way up to the most heinous types of exploitation, things associated with human trafficking, child exploitative material and that sort of thing.

In the context of social media and young people, what's the government's role in terms of developing regulations? What is the role of social media platforms in terms of trying to create frameworks that deal with the massive range of possible challenges that we face here?

There's about a minute and a bit left, and I know it's a big question. Hopefully, that's enough time for you to give some feedback to the committee.

Dr. Emily Laidlaw: Thank you.

It's an enormous question, but it's the money question.

I will keep it brief and state that it's crucial that government play a role, because thus far we've mostly relied on corporate self-governance and it hasn't worked. I mean, we're seeing all kinds of harms happen online.

What we do need is a regulator, because a regulator can be more agile in dealing with this. It's too cumbersome for some of these concerns to work through the courts. We need help to sort of set practices. Each platform is different, so the platforms really do need to come up with solutions for their spaces. It's just that there needs to be a method to hold them accountable for it. They need to demonstrate to some regulator the steps they're taking to protect children.

I think we need to divvy up the harms. If you're talking about specific child protection measures—looking at child sexual abuse images, intimate image abuse, trafficking—these are crimes, and there are the primary actors who, to the extent they can be found and prosecuted, should be the targets, but there is a separate responsibility and special duties that should exist for platforms.

When it comes to child—

● (1620)

The Chair: Thank you, Ms. Laidlaw.

I'm sorry. The worst part of my job is cutting people off.

Ms. Khalid, you have six minutes. Go ahead, please.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you very much, Chair.

Ms. Laidlaw, you talked about solutions with respect to social media companies. Perhaps you can finish your thoughts on Mr. Kurek's question and, as well, comment on what you think are good solutions on this that social media companies can look into and can have best practices for.

Dr. Emily Laidlaw: Just to clarify, are you asking from a corporate governance perspective or what laws we should pass?

Ms. Iqra Khalid: I meant both, actually.

Dr. Emily Laidlaw: Okay.

First, this is a legal question and we do need the government to pass online harms legislation, because it needs to set the duties for companies. Basically, it needs to set minimum standards. The companies themselves, though, can start taking more seriously protecting children from harms.

I think one of the issues is that a lot of the transparency we're seeing now tends to be more of a marketing exercise. I think it's not as upfront about what some of these practices are. This is a key aspect, of course, that Dr. Caraway has talked about: the attention economy.

Specifically for children, I think we need to think about this as mind manipulation. Historically, there were interventions in areas of advertising to protect children from mind manipulation. You didn't have certain ads at certain times of day and with children's shows. This is the same thing that's happening on social media: pushing suicide content, eating disorder how-to content and so on.

It is critical that these platforms, from a design basis.... How are we designing this platform? How are algorithms pushing content? How are we nudging certain behaviours? They need to address that and account for that, so I think there should be special duties for children.

Ms. Iqra Khalid: Thank you very much.

Dr. Caraway, do you have any comments around the remarks from Ms. Laidlaw with respect to where the economy is versus mind manipulation or changing the behaviour of consumers? What role does government have to play in that with respect to regulation? I realize and understand that we can't just create regulations where bad actors don't always follow the regulations. What role do you think government has to play in that balance of economy, efficiency and mind manipulation?

Mr. Brett Caraway: One thing that I think is really important...well, there are kind of two things.

I think we need to pay very careful attention to what constitutes informed consent. What is problematic to me is the way in which not just children but also everyday users are confronted with end-user licence agreements that require someone like Dr. Laidlaw to make sense of them because they are so convoluted. They require so much expertise and are subject to change almost on a daily basis. I think it's important to revisit what actually counts as consent here.

Then there is transparency and the way in which the data is used. This is something where I do think that you need to be able to have something like a Privacy Commissioner, who can send in a third party auditor to see what's actually happening behind the scenes.

Lastly, I would say that the penalties have to have bite to them. Yes, $25 million sounds like a lot, but maybe not to Meta or Alphabet, while 5% of global revenues sounds a little more serious. I like that sort of approach too.

● (1625)

Ms. Iqra Khalid: Thank you.

We've seen, over the past number of years, social media being used as a platform for advocacy, for speaking out and expressing yourself, not only across Canada but also across the world. A couple of years ago, on TikTok, we saw a young woman putting on makeup and talking about issues in order to circumvent the algorithms on what was being said or what was being displayed.

Where is that interlink between social media and freedom of expression and making sure that kids in Canada have the safety and security they need as they navigate through this space as well?

Mr. Brett Caraway: Who would you like to respond to that?

Ms. Iqra Khalid: I would like your comments first, Dr. Caraway, and then I'll go to Ms. Laidlaw.

The Chair: We have roughly a minute. Go ahead, Mr. Caraway.

Mr. Brett Caraway: Since that bears on freedom of expression, Dr. Laidlaw would maybe want to take that one, instead of me.

Dr. Emily Laidlaw: Thanks, Dr. Caraway.

I will say that freedom of expression is foundational. If you pass a law that just incentivizes a focus on harms, you incentivize companies to put in rudimentary solutions that, in fact, backfire. There's been a lot of evidence of backfiring, where what ends up being silenced is racialized and other marginalized voices.

For the requirement on companies, if we care about harms, we care about harms to rights, so it needs to be a dual focus that social media companies have. They need to focus on how they protect and promote freedom of expression and show that to a regulator. They need to demonstrate the steps they are taking that are contextual and bespoke to their services.

Ms. Iqra Khalid: Thank you very much.

My apologies, Dr. Laidlaw. I didn't address you as I should have. That's my bad.

Dr. Emily Laidlaw: I didn't even notice, but thank you.

The Chair: Thank you, Ms. Khalid.

[*Translation*]

We now go to Mr. Villemure.

[*English*]

Before we continue with Mr. Villemure, I want to make sure that our guests have their interpretation on, if they need it.

[*Translation*]

Go ahead, Mr. Villemure. You have six minutes.

Mr. René Villemure (Trois-Rivières, BQ): Thank you, Mr. Chair.

Thank you to our two witnesses for being here today. Their reputations precede them.

I'm going to start with Ms. Laidlaw.

You aren't a fan of self-regulation, are you?

[*English*]

Dr. Emily Laidlaw: No, I am not, but I am a fan of giving room to the companies to come up with the solutions themselves.

[*Translation*]

Mr. René Villemure: If I asked you today to set up a regulator—hopefully, not the CRTC—what would you recommend?

[*English*]

Dr. Emily Laidlaw: I recommend that we create an online safety regulator and that they have an obligation to investigate companies and to audit companies for their compliance with specific duties. I think the duty should be a duty to act responsibly with, perhaps, a special duty of care to children.

I think the regulator should also have a very important education role with the public. We have realized that so much of this is about lifting up the capacity and understanding of the public, and also holding companies accountable.

[*Translation*]

Mr. René Villemure: Would that regulator be similar to the Conflict of Interest and Ethics Commissioner or the Commissioner of Lobbying? In other words, would the regulator be someone appointed by Parliament, or would it be a public servant in a department?

[*English*]

Dr. Emily Laidlaw: I think it's absolutely crucial that this regulator is independent from government. It would be more akin to the Privacy Commissioner because you would be creating a digital human rights regulator. They need to be independent from any pressure when it comes to how to balance rights. It needs to be through a legal lens and a corporate accountability lens. Also, there needs to be the power to impose quite hefty monetary penalties, as Dr. Caraway mentioned.

● (1630)

[*Translation*]

Mr. René Villemure: Precisely. Earlier, someone said the penalties should be a percentage of the company's revenues, as opposed to a $25,000 fine, which is trivial under the circumstances.

You talked a lot about education, as have all the witnesses we've heard from, including police officials. Ultimately, though, no one has said who should educate who. Perhaps the new regulator should have a mandate to provide that education, even in schools, since we are talking about young people.

What does that education look like to you? Everyone is in favour of education, but no one has put forward a solution as of yet.

[*English*]

Dr. Emily Laidlaw: I think it's crucial that it's through the regulator, and we've seen this in Australia with their eSafety Commissioner. I think that would be the model here for a regulator and educator.

I think partly it's that the education across the country and in different schools and communities varies greatly, and it depends on people reaching out for the information. It depends on schools bringing in the right people. At the moment, there is a lot of just scaring children or parents, and most of the studies show that's ineffective. I've tried to say that to my children's school, and they've been really receptive.

I think education is so core to this that the regulator needs that as part of their mandate.

[*Translation*]

Mr. René Villemure: The regulator should have the authority to go into schools to deliver that education. Is that right?

[*English*]

Dr. Emily Laidlaw: That's an interesting question about federal-provincial powers that certainly could set the curriculum and provide the resources that would hopefully influence different schools and even municipalities and what they're implementing and so on. I guess the hope is that this will trickle down. Ultimately, there is a provincial aspect to this, so if we start seeing provincial regulators appear, then maybe they could work together, much like the way we have seen with the privacy commissioners.

[*Translation*]

Mr. René Villemure: I am a staunch advocate of respecting provincial jurisdiction.

You said Canada was a laggard in digital legislation.

Is it too late?

I'm quite familiar with the European law. We can try to catch up, but is it too late?

[*English*]

Dr. Emily Laidlaw: We're not too late now, but we will be soon if we don't introduce laws. Europe and the U.K. just passed their online safety legislation—the Digital Services Act—earlier this year or in the last year, and they're in the midst of implementing it.

If you fast-forward five years, what I think we're going to see is more coordinated global investigations of companies, which takes care of some of the cross-border issues. If Canada doesn't move on this in the next year or so, I think they will fall woefully behind. However, right now we do have a late-mover advantage.

[*Translation*]

Mr. René Villemure: In 30 seconds, can you tell me whether you support Bill C-27 as it currently stands?

[*English*]

Dr. Emily Laidlaw: I fully support the recommendations for amendments by Commissioner Dufresne regarding Bill C-27. I think it needs to be amended. I think it only solves part of the problem, because it's still a consent paradigm. Also, as long as it relies on consent, it doesn't dive into some of the more problematic aspects of social media and their influence, which, really, nobody can consent to.

Therefore, unless we wholly change Bill C-27, which I don't think we'll do, we need online harms legislation. I do think the AI act is problematic and needs to be pulled out of Bill C-27 and reworked. It absolutely should not be set up under ISED as a commissioner within that body.

[*Translation*]

Mr. René Villemure: Thank you very much.

The Chair: Thank you, Mr. Villemure.

[*English*]

Being aware of the time and the votes, what I am thinking—and I want you to think about this as well—is that we can go six minutes with Mr. Green. We're going to need some time to switch over to the next panel. We could have the opening statements. I expect we're going to have two opening statements in the next panel.

That would take us roughly up to the time of the votes, but it would end this round after Mr. Green. I would encourage our witnesses to submit any additional thoughts they may have.

Mr. Green, go ahead for six minutes, please.

Mr. Matthew Green (Hamilton Centre, NDP): Thank you very much, Mr. Chair.

I want to pick up on some of this, particularly around Bill C-27. I myself think that this portion of the bill would have been better dealt with here under an ethical framework rather than an industry one.

Dr. Laidlaw, can you maybe talk about the ethics of AI and why, from a legal framework, those considerations in terms of the legitimacy of democracy and the ways in which AI is undermining society would probably be best situated as a carve-out, as you just suggested?

● (1635)

Dr. Emily Laidlaw: That's a great question. Thank you.

I think we have seen, just in the last year, the way AI has transformed our society, and we're just at the beginning of that journey. The problem with the AI act, as it stands right now, is that it's not sufficiently developed to be able to actually cope with the different problems we're going to face. It needs to be carved out so that we can actually sit down and have a proper discussion about the ways in which AI can be used that fundamentally will disrupt democracy, interfere with our ability to make decisions and create physical risks to us individually or collectively.

We need to break down those various risks and the opportunities and draft a legislation that reflects that. I think we do have a model, as well, in Europe that can help us. However, as it stands, the AI act must be amended.

Mr. Matthew Green: I want to get more specific.

You referenced the undermining of democracy. I'll reference the case of Cambridge Analytica, where we know that Facebook did not undertake sufficient oversight to ensure that the use of data was done according to its own terms of service.

I think I heard in your testimony that having the industry regulate itself is a problem, although it might be able to present some solutions.

How confident should we be that social media companies have a full grasp of how their data is being used and whether the data is being properly protected? Further to that, do you think they know and just perhaps allow it to happen anyways?

Dr. Emily Laidlaw: I think it's a bit of both. I think they are not providing the full picture. I do not think they fully know what is happening.

For example, a colleague of mine, Joel Reardon, has done some reverse engineering of various apps that say they put in place all the child protection measures. What has been revealed through this is that many apps have not.

Essentially, we're relying on people finding this out and then having a scandal. That's just woefully insufficient here. Transparency on its own is meaningless. We actually need some sort of avenue to investigate, audit and lift the lid on these companies. Otherwise, we end up with a crisis like Cambridge Analytica.

Mr. Matthew Green: Let's go back to that.

In your opinion, are there ways, through legislation and regulation, that the federal government could do a better job of protecting the personal information as collected and used by these platforms?

Dr. Emily Laidlaw: I think one thing we need to look more closely at is what the no-go zones are. There are actually certain forms of collecting data that should be seen as wholly inappropriate. I think we still rely so much on consent that it has—

Mr. Matthew Green: Can you give us a couple of examples, for the purpose of your testimony?

Dr. Emily Laidlaw: One example might be just the terms and conditions on social media. We will agree to the harvesting of all kinds of data for whatever purposes because we want to use that app. Most of the studies show that what we're all undergoing is privacy fatigue, where we essentially know it's bad for us, but agree to it anyway. This is really paternalistic and this is the problem. Essentially, what we're saying is that people shouldn't be agreeing to this because they don't really understand what they're agreeing to. It's then being sold on to data brokers, which Dr. Caraway talked about, and then we lose control. We don't actually know what happens to the data.

California does a better job, with its law, of basically saying you need to be able to track that data and who it all goes to. If you rely on consent, you can withdraw that consent and know where that data goes. All those are avenues to data protection and privacy laws.

Mr. Matthew Green: That's very helpful and it gives me a good segue to Mr. Caraway.

You mentioned that some social media apps take a drift net approach to data collection. Are you able to discuss which apps take this approach and whether or not our current legislation provides sufficient protection?

Mr. Brett Caraway: A lot of data is harvested by even the most prominent social companies. This is everyone from Facebook...I would include Google, Instagram and TikTok. They'll collect everything that you post—that's all of your personal data—and they'll also track all of your so-called transactional data and interaction data.

Facebook is successful because it's able to leverage your social connections at scale. Google is successful because it can leverage your purchasing intent at scale.

Mr. Matthew Green: When you say “at scale”, for the purpose of the public and the testimony, what do you mean?

● (1640)

Mr. Brett Caraway: They can take this information, use it in a digital context, package it with almost zero marginal cost and then sell it to data brokers.

The Cambridge Analytica thing is a great example, because actually the initial data harvesting that happened didn't violate Facebook's terms at the time. They had a reciprocal data exchange agreement in place. It was only when the This Is Your Digital Life app shared it with Cambridge Analytica that the actual scandal happened, because that's how they—

Mr. Matthew Green: I have 20 seconds left.

Do you know of any restrictions on how data can be used? Can we as individuals limit or find out how our data is being used?

Mr. Brett Caraway: Most of the provisions right now are the same old things that have been in PIPEDA since the year 2000, I suppose, which is why we're now revisiting it.

The thing we need right now is an enumerated right to privacy that's part of a legal test when you're thinking about an injunction or a fine.

Mr. Matthew Green: That's very helpful.

Thank you.

The Chair: Thank you, Mr. Green. I'm glad you were keeping track because we hit the wrong button on the phone and lost track. You could have had another two minutes if you wanted.

First of all, I want to thank our guests for appearing today. As I mentioned earlier, if there's any other information that you would like to submit to the committee in consideration of this report, please do so, to the clerk.

I want to apologize, first and foremost, for the disruptions today and for the disruption last week. I wasn't feeling well. I appreciate your patience in coming back to committee this week and sharing the information that you did.

Thank you, Ms. Laidlaw and Mr. Caraway.

We're going to suspend for a couple of minutes. We're going to come back with our new panel and provide opening statements. We have a bit of time for that, so let's suspend for a minute or two.

Thank you.

● (1640)

_____(Pause)_____

● (1645)

The Chair: We're going to resume the meeting. I'd like to welcome everyone back.

I'd now like to welcome our witnesses for the second part of our meeting today.

As an individual, we have Mr. Matt Malone, assistant professor at Thompson Rivers University. Welcome, Mr. Malone. From The Dais, we have Sam Andrey, who is the managing director; and Joe Masoodi, who is a senior policy analyst.

Just to advise you, we are under an indication of votes. We have about 27 minutes, so we're going to start with opening statements. We'll suspend the meeting and then we're going to come back for Qs and As. I appreciate your patience with this.

Mr. Malone, you have up to five minutes to address the committee.

Go ahead, sir, please.

Mr. Matt Malone (Assistant Professor, Thompson Rivers University, As an Individual): Thank you, Mr. Chair.

My name is Matt Malone, and I am an assistant professor at Thompson Rivers University faculty of law in Kamloops. Today I am attending the meeting in a personal capacity.

I am going to use my opening remarks to share my thoughts using a case study, which is specifically regarding the selective ban of TikTok on government-issued devices that was announced in February 2023. As the committee might recall, that selective ban was accompanied by a statement about concerns relating to privacy and security.

These stated concerns do not explain several things. First of all, they do not explain why the government waited five months to act on the underlying intelligence brief that warned about TikTok's practices. Second, they do not explain why the government continues to buy advertising on TikTok itself. Finally, they do not explain why the government has ignored that TikTok is not the only app that retains user data in foreign jurisdictions and potentially shares it with foreign regimes.

As the Treasury Board Secretariat confirmed to me a couple of days before this hearing, none of the following apps are banned from download and use on government-issued devices: the Russian-affiliated VKontakte social media app, the Russian-affiliated Yandex app, and the Russian-affiliated Mail.ru app, as well as other social media apps, like Facebook, Instagram, Tinder, Snapchat, Bumble, Grindr, Truth Social, Gab and Discord, which was implicated in the 2022-23 Pentagon leaks and which Dr. Laidlaw noted does not have child safety protection measures in place.

As I recommended in a recent article—and as I'll take this opportunity to recommend again now to the President of the Treasury Board—I believe that a better privacy and security baseline would see the government ban all social media apps on government-issued devices, unless there is a strong business justification otherwise. It's crazy to me that the apps I just listed are not banned on government-issued devices. I also believe that the government should stop buying ads on all social media services.

Even with such bans in place, it is worth noting that federal privacy law places no meaningful constraints on data transfers to jurisdictions like Russia and China. An internal government brief that I obtained through the Access to Information Act notes that Bill C-27 and the proposed privacy legislation currently before Parliament avoided putting into that bill any new or European-style restrictions on the transfer of personal information across borders specifically out of deference to commercial interests. It's very telling that the privacy bill before Parliament is being stewarded by the industry portfolio in cabinet, not a portfolio in human rights, public safety or national security.

Like many social media apps, TikTok does deserve opprobrium for its privacy violations, data harvesting and narrative control practices, and for granting access to data despite assurances otherwise. Like other social media apps, it is a vector for online harm visited on young people. Its business model is focused on privacy-invasive, targeted advertising that exacerbates the mental health crisis affecting young people. The app's safety features for children are all easy to bypass.

Through various access to information requests, I have seen several internal briefings where Canadian government actors repeatedly identified these problems. I'm happy to talk about these.

However, it's important to note that the real culprit here is Canadian law, because it does not stop these practices for TikTok or any other social media service. As TikTok lobbyists appearing before this committee repeatedly underscored, TikTok's handling of Canadians' user data is governed by Canadian law. That's the problem. Canada's privacy laws fail to respect the rights and interests of individuals and collectives in the digital age. Enforcement is basically non-existent. At the federal level, the Office of the Privacy Commissioner has become skilled at making fanfare announcements about its investigations, but it is very slow at investigating, as I learned in my own complaint about the ArriveCAN app, which was ultimately sustained.

Law enforcement has struggled to adapt to the new digital landscape as well. The RCMP's national cybercrime and fraud reporting system, which this committee recently heard about in glowing terms as part of this study, is actually two years behind schedule and still in beta testing. Its website says that it accepts only 25 complaints per day nationwide.

To give members another illustrative example, as I learned in a recent access to information request, the RCMP's cybercrime investigative team has only eight employees in all of Alberta. Here in British Columbia, where there was a recent tragic sextortion case involving a young person that was carried out over social media, there are only four employees on the cybercrime investigation team for the entire province. There are none in Saskatchewan, Manitoba or any of the maritime provinces.

With privacy and data protection legislation that deprives citizens of meaningful protection, government funding priorities deeply out of alignment with stated values and actual needs, and gaps in law and policy that the government shows no urgency to fill, the federal government's policies and practices pose significant challenges to addressing the real types of harms that we are seeing perpetuated these days on social media.

● (1650)

To wrap up, I want to thank the committee for its unexpected invitation.

I also want to give a particular shout-out of appreciation to the MP for Mississauga—Erin Mills for her leadership on this very important issue. I've been very impressed with her work on this file.

I look forward to answering, to the best of my abilities, any questions that the committee members might have.

Thanks.

The Chair: Thank you, Mr. Malone. We certainly appreciate your kind words about our honourable colleague.

Mr. Andrey and Mr. Masoodi, I understand that you're going to split your time. You have up to five minutes. Whoever wants to start, go ahead, please.

Mr. Sam Andrey (Managing Director, The Dais): Thanks very much.

Thanks for the invitation to share our perspectives on this important issue.

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

I have my colleague Joe Masoodi here with me. Together with our former colleague Yuan Stevens, we published a report three years ago called “Home Ice Advantage”, which examined the subject before the committee today, the transborder data security of social media platforms. While a lot has changed in the last three years, the core challenge of inadequate protection for Canadians remains.

Mr. Joe Masoodi (Senior Policy Analyst, The Dais): Social media platforms collect, transfer and store a wide variety of personal and sensitive information, including personal identifying information, private messages, location, financial information and biometric data. These platforms have been purposefully designed to keep individuals online and engaged to reap as much data about them as possible. Through the aggregation of this data, it is possible to create detailed profiles and inferences about individuals, including their political opinions, sexual orientation, religion, income, health, or details about their families. This is true of TikTok but also of most major online platforms.

Despite the significant risks to Canadians through the potential misuse of this data, there are currently inadequate protections over how Canadians' personal data is transferred and stored, particularly outside of Canada. This threatens Canadian sovereignty and the digital security and privacy of Canadians. Personal data can be accessed by national security and law enforcement agencies in countries without sufficient legal protections, such as China. I think it is also worth adding that technology companies can experience buyouts, mergers and bankruptcy that can change where and how personal data is stored and the privacy protection it receives. Finally, malicious actors can always take advantage of data with insufficient safeguards.

● (1655)

Mr. Sam Andrey: In our annual survey of online harms, we found that Canadians have very low trust in social media platforms, both to keep their data secure and to act in the best interests of the public, ranking well below other technology companies and other organizations of a variety of types. In fact, trust in TikTok, specifically, fell significantly last year, to last place. Only 7% of Canadians say that they have a high degree of trust in the platform, despite its rapid growth with nearly 30% of Canadians using the platform.

TikTok has been the subject of particular scrutiny, given its corporate structure. As was pointed out earlier in the committee, prior to 2019, TikTok's privacy policy was transparent in stating that it shares people's information “with any member or affiliate of [its] group” in China. This line was later updated to remove that specific location reference, but the sharing provision remains. That same provision is also in the privacy policy of WeChat, which is used by 6% of Canadians. As our colleague Mr. Malone has pointed out, it is true of many others.

Canada's current privacy law does not prohibit companies from transferring personal data to third parties or outside of Canada in this way. We think that there is an opportunity before parliamentarians to respond to these risks through the proposed Bill C-27. However, as it currently stands, Bill C-27 would, in some ways, allow for even easier data sharing to take place between corporate actors by eroding what limited consent provisions do exist. Proposed section 18 of the CPPA creates new, large carve-outs for companies to share data without either knowledge or consent through the inclusion of language like “business activities” and “legitimate interest”.

We don't think that it should be the exclusive responsibility of Canadians to educate and protect themselves online. We would propose that there be more precise requirements added to the bill to ensure that equivalent levels of protection are provided for data when it's transferred outside of Canada. We would also suggest requirements that near the EU's GDPR, to obtain explicit informed consent from Canadians for the transfer of their personal data to jurisdictions that do not provide equivalent levels of protection, providing information about both the specific countries involved and the specific data. While a lot of people have pointed out to this committee that there's consent fatigue, we, at least, think that transparency with respect to data transferred to countries outside of Canada is important.

We'll end by saying that Canadians overwhelmingly support such a change. A representative survey that we conducted found that 86% of Canadians support requirements to keep Canadians' data in Canada, with only 3% disagreeing.

Thanks for your time. We look forward to your questions.

The Chair: Thank you, Mr. Andrey and Mr. Masoodi.

[*Translation*]

We now go to Mr. Gourde for six minutes.

After that, we will have to suspend in order to vote.

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

This question is for all the witnesses.

Canadians expect their government to protect them from the digital platforms. When it comes to digital legislation, many witnesses have told the committee that Canada is behind European countries and others.

Because we are so behind other countries, do you think we need to move pretty quickly to, at the very least, update our laws?

[*English*]

Mr. Matt Malone: I'm happy to jump in.

I believe one of the problems that Canada faces is that we're not a large power and we're stuck between approaches to privacy and data protection among large powers that are diametrically opposed. Failing to act soon will lock us into one of those approaches. The Europeans have adopted a more restrictive approach. Ever since the drafting, passage and implementation of the GDPR, we've seen an array of restrictive measures, which are leading to things like data localization, stricter requirements around data transfers, and a robust equivalency test.

The United States is taking a diametrically opposed approach with its regulatory framework, in which it has not updated its privacy legislation, and there's no uniform privacy legislation in the United States. At the same time the U.S. is doing that, it's exporting, through trade treaties and governance bodies worldwide, a view of data governance and privacy that locks in what Canada can do.

Discussions about data transfers have to take into consideration the fact that the Canada-United States-Mexico agreement has a prohibition on restricting cross-border dataflows, and it has other restrictions that are relevant as well. The CPTPP has similar restrictions.

One of the problems with Canada's failure to act is that we're getting locked into one of these approaches. Unfortunately, we show no urgency around acting. The Privacy Act, which regulates government conduct, hasn't been updated in over 40 years. PIPEDA is well in need of a meaningful update, not just tweaks. I personally don't believe that Bill C-27 is the appropriate way to do that.

I'll let the other panellists chime in.

● (1700)

Mr. Sam Andrey: I would add that I agree with the premise of your question, that we are falling behind in some respects, though I think we have, as Dr. Laidlaw put it, second-mover advantage to learn from some of the lessons and some of the flawed legislation or approaches that have been passed in allied jurisdictions.

On AI regulations specifically, I think Canada is moving quickly as relates to the rest of the world, which I think is a good thing, but, yes, I would say we need to move more quickly, and Bill C-27 is part of that.

[*Translation*]

Mr. Jacques Gourde: Mr. Malone, you said the RCMP lacks investigative capacity. We heard from RCMP officials who seemed to say that they had the resources to carry out investigations. Of course, they didn't specify whether they had the capacity to carry out multiple investigations at once.

Are you really concerned about the RCMP's lack of investigative capacity?

[*English*]

Mr. Matt Malone: When you look at the resources that are available, they're not meeting the demand. In 2018, when Public Safety went through a cybersecurity update and threw a lot of money at the RCMP to get more serious about online cybercrime, that was when the initial announcement was made about NC3, the national cybercrime coordination centre.

I wrote about this three years ago and said that we were already waiting a long time to get this rollout happening, but fast-forward three years, and that reporting system is two years behind schedule. If you visit the website right now, it will tell you that the system is still in beta testing and that it accepts only 25 cybercrime complaints a day for the entire country, which is really low. In a series of access to information requests regarding the number of resources that were devoted in terms of personnel, I discovered that there are several provinces that don't have any cybercrime investigators, which is a really shocking statistic. Here in B.C., the third-largest province in the country, we have only four full-time people on the cybercrime team.

I believe these tools need to be rolled out more rapidly. There should be more transparency around them, and legislation should be crafted around what we're seeing, because these tools allow us to understand what types of harms are being perpetuated. There are all kinds of analyses you can run based on the reporting data that comes in, and NC3 shows that more than half the reports that go to NC3 are about ransomware. It's really interesting that Canadian legislation ignores ransomware, which is the biggest cybercrime threat we're facing.

One thing that's interesting to take into consideration when we talk about Bill C-27 is also Bill C-26, which would regulate things like ransomware for critical industries.

[*Translation*]

Mr. Jacques Gourde: I'm almost out of time, Mr. Malone.

Given the results, do you think the government is investing enough in the RCMP to ensure data security on platforms, or not enough?

[*English*]

The Chair: Please provide a very quick response.

Mr. Matt Malone: I think there isn't enough money given to the RCMP in this area, frankly.

[*Translation*]

The Chair: Thank you.

Thank you, Mr. Gourde.

[*English*]

Next, we have Ms. Khalid, for six minutes.

Ms. Iqra Khalid: Thank you very much, Chair.

Thank you to our witnesses for coming before us today and shedding light on this very important issue.

Mr. Malone, I'll start with you. We had representatives of TikTok come to our committee, and we learned from them that the majority of Canadian data is actually not stored in Canada. It is stored elsewhere across the world, including Malaysia, Singapore, etc. What are the legal implications of that with respect to Canadians' privacy rights?

● (1705)

Mr. Matt Malone: Thanks for the question.

I think it's really important to identify the TikTok representatives who spoke as lobbyists. They're registered lobbyists, and they do lobbyist work. I think it's important to talk about how a lot of the claims they made were very disingenuous. There are easy bypasses around a lot of the safety controls for children that they vaunted.

TikTok has been caught—to respond more directly to your question—engaging in all kinds of worrying conduct with respect to user data. There is public reporting that talks about TikTok accessing physical locations of journalists who are using the app, in order to track down their sources. That's in the public domain. There is public reporting about TikTok directing user data from the United States through China despite assurances otherwise, and there's a raft of other reporting.

There's internal government reporting from Canadian government actors like the Privy Council Office's intelligence assessment secretariat that identifies all kinds of other problems around the type of data and the persistent collection of data that occurs through the app. There are also materials that I've seen from the cyber-threat intelligence unit at the Canadian Forces intelligence command at the Department of National Defence that identify a series of concerning problems around censorship and so forth.

One of the really difficult issues here is that Canadian law is very permissive when it comes to data transfers. Even if you look at the proposed privacy legislation, Bill C-27, there's essentially nothing that would stop data transfers outside of Canada. Certainly, the privacy notice for TikTok states that by using TikTok you accept the terms and conditions, which are that the subsidiary TikTok can share that data with its corporate body, ByteDance, and Canadian law lets that happen. Even the proposed Canadian law would let that happen. Proposed section 19 and proposed subsection 11(1) of Bill C-27 specifically permit this type of data transfer.

Canadian data transfer law is essentially premised on the idea that organizations can send data to other organizations if they deem the protections are sufficient or adequate, as they would be in Canada. This approach is really different from the European approach, which is jurisdictionally grounded—country to country. You can't transfer data outside of a country unless you're satisfied that the protections would be essentially equivalent. There's a really big difference in Canadian data transfer law compared to the European data transfer law. Once data gets out of Canada, there's really no telling what happens to it. They don't take basic safeguards like you do.

For this meeting, I asked the chief information officer of the House of Commons where the data was being localized and processed for Zoom, which I would be using, and I was told—and I was very happy and impressed by this—that the data would be processed in Canada. Your in camera meetings are even more secure, so good on you. It's not for the users of TikTok.

Ms. Iqra Khalid: Thank you. I appreciate that.

In previous interviews, you've talked about power imbalances with users and the collection of vast amounts of data. What did you mean by that? Can you expand on that a bit for us?

Mr. Matt Malone: Like many folks who have appeared before this committee and committees dealing with related topics, I have a lot of concerns about how these power imbalances affect users' ability to offer consent that is meaningful and that is informed. When you click “accept” on a very length privacy notice, your ability to offer or provide consent is really challenged when the power imbalances that exist are such that you are an individual user and the company that might be collecting the data might have a market valuation that exceeds the size of a G7 country.

Ms. Iqra Khalid: Thank you very much. I really appreciate that.

Mr. Andrey and Mr. Masoodi, you've authored or contributed to a report that has surveyed online harms in Canada as it relates to social media platforms in the public square. Can you tell us a bit more about the key findings of this report and speak specifically about the way vulnerable marginalized communities and groups are targeted online?

Mr. Sam Andrey: Sure. I'm happy to.

Joe, feel free to jump in here.

We do an annual survey of a representative group of Canadians to track, basically, Canadians' experiences online with harmful content or illegal experiences. At a high level, we start with hate speech: 40% of Canadians say they see hate speech at least monthly, and about 10% of Canadians say they have personally been targeted by online hate speech. Those rates are about double or triple for a variety of marginalized communities and racialized communities. It would be about double that rate for 2SLGBTQ Canadians, and three times that rate, or 30%, say they have personally been targeted with hate speech. There's a tracking of that.

We also track exposure to, and belief in, misinformation and disinformation. We have Canadians do a quiz, basically, of a series of true and false statements. We find that about 15% of Canadians we assess as having a high degree of belief in misinformation. Those Canadians are more likely to say they consume their news on social media and are less trusting of mainstream media sources.

● (1710)

The Chair: Mr. Andrey, I'm going to have to stop you there, sir. I apologize for that.

[*Translation*]

We are going to suspend for voting. When we get back, it will be Mr. Villemure's turn for six minutes.

[*English*]

It should take about 15 minutes or so before we're back, so I appreciate your patience.

Thank you.

The meeting is suspended.

● (1710)

_____(Pause)_____

● (1730)

The Chair: Welcome back to the meeting.

[*Translation*]

We will now begin the round.

Mr. Villemure, you have six minutes. Please go ahead.

Mr. René Villemure: Thank you to the witnesses for being here.

Mr. Malone, it's a pleasure to see you back here.

Is informed consent impossible, in your view? Is it pointless? Is it a mirage in today's world?

Mr. Matt Malone: I think the word mirage accurately captures the current state of affairs.

[*English*]

I think informed consent, which is what all Canadian privacy laws are currently based on, doesn't serve the ends that we really need data protection and privacy law in this country to serve. The reality that Bill C-27 has perpetuated this—the idea that this instrument will still work and still serve its ends even with the legitimate business exceptions, even with the rules around implied consent—really won't take us to a place where we have robust privacy and data protection law in this country.

I think you need to fundamentally shift the paradigm so that possessing, retaining, using or disclosing personal information becomes a liability, as opposed to a profitable way to run a business, which is what we have let these ad exchanges/social media companies do.

[*Translation*]

Mr. René Villemure: That's a very good way to look at it. As I see it, free and informed consent, as they say in medicine, is never free if you want to access whatever it is. Informed consent is a fiction, or even a mirage.

You also said that Canada is a middle power in this area. That's particularly true vis-à-vis the European Union, the U.S. and China.

What hope does Canada have of playing a role and carving out a credible place for itself through its legislation?

[*English*]

Mr. Matt Malone: I think Canada has an opportunity to reclaim a bit of the traditional role that we like to see Canada have, which is serving as a middle power with allied states.

Several ideas have been floated around creating safe dataflow zones that map onto the security alliances that already exist, like NATO for example. We already have a commitment to mutual defence with our NATO allies. It would seem logical that we might feel comfortable sharing our data, our personal information, with these allies in a free cross-border dataflow zone. There are opportunities for Canada to certainly create a niche role when it comes to regulation and the creation of regulatory frameworks for cross-border dataflows.

I think the more appalling concern that I have is with the state of the current law. The fact is that a lot of Canadian law, and certainly the priorities of legislators right now, is to create privacy law that applies only to the private sector. I think one of the real problems we've seen—and we saw this through the pandemic as well—is that we need robust privacy and data protection laws that also apply to government. I've been really upset at the fact that the artificial intelligence and data act does not apply to government actions, which is really concerning when you think about the deployment of AI technologies, AI-fueled and AI-driven technologies such as the ArriveCAN app.

I've also been really concerned about the fact that the priorities with Bill C-27 have not focused on government. To me, it's disturbing that this effort has been led by the industry portfolio and Bill C-27 would create new regulatory instruments that would be answerable to the Minister of Industry. It's really hard to say that we're approaching privacy from a human rights or law enforcement or national security perspective when the bodies we're creating are not truly independent. Not only are they not truly independent, but they're subservient to an industry portfolio whose mandate is to grow the economy.

[*Translation*]

Mr. René Villemure: I share your concerns, believe me.

Mr. Andrey, I have the same question for you.

Canada is a middle power, between the European Union and the U.S. or China.

What could Canada propose that would be seen as acceptable?

● (1735)

[*English*]

Mr. Sam Andrey: I honestly echo a lot of what was just said. I think there's an ability to build on...and maybe I'll speak specifically with respect to online harm legislation. Germany was the first mover and basically created a 24-hour takedown regime. The outcome was an over-censorship response from many of the large platforms. They didn't want to deal with the liability, so they removed too much lawful expression.

We have an opportunity to learn from mistakes like that.

[*Translation*]

Mr. René Villemure: Since time is running out, I'm going to interrupt to ask you to please send the committee some information on what happened in Germany. That would be very appreciated.

I have one last question before I'm out of time.

Do you see a role for an independent regulator, along the lines of the Conflict of Interest and Ethics Commissioner, the Privacy Commissioner or the Commissioner of Lobbying? Conversely, do you think it should fall under the scope of a department like Innovation, Science and Economic Development Canada, as is currently proposed? Where do you see that regulator? What powers should it have?

[*English*]

Mr. Sam Andrey: I see a role for a digital regulator.

Currently, there's the idea of having an AI data regulator in Bill C-27, but it's an ISED department official. This, I think, is unacceptable, especially given that the minister will have the competing roles of championing the economic benefits of AI and regulating its risks. At a minimum, they should be appointed by the GIC. Ideally, it would be a parliamentary appointment that is separate.

I think you could task the same regulator with the online harms portfolio. It could be two, but that's a lot of digital regulators. That regulator would have the power to do audits and a forum on ombudsman-type functions to support individuals. They would also have a transparency function.

[*Translation*]

Mr. René Villemure: It would be an independent regulator, then.

The Chair: Very good.

Thank you, Mr. Villemure.

[*English*]

Mr. Andrey, thank you.

Mr. Green, you have six minutes. Go ahead, sir.

Mr. Matthew Green: Thank you very much.

I know there was a shout-out to start the round of testimonies. In the spirit of shout-outs, I want to give one to Christelle Tessono. I understand she is now in policy and research at The Dais. I know her work has been reflected in previous committees, as well as in some of the deep dives I have taken into this field. The technology is often far ahead of the scope of our subject matter expertise, so having subject matter experts like yourselves is incredibly important. I appreciate your being here today. I appreciate any contributions that she may have made, as well.

I want to begin with Mr. Malone.

In a September 2023 article, you mentioned you reviewed a federal government document entitled “Economic Security and Technology: TikTok Takeover”. Are you able to highlight the concerns raised in that report, and do you share those concerns?

Mr. Matt Malone: I'm not sure what document you're referring to.

Are you referring to the document that informed the piece for my recommendation to ban all social media applications on government-issued devices?

Mr. Matthew Green: That's correct.

If you've been following the study, you will have noted I have been very adamant about expanding the scope of regulation, oversight and scrutiny to all platforms, not just TikTok.

If you care to comment on that, it would be helpful.

Mr. Matt Malone: The document comes from National Defence and their cyber-threat intelligence unit. It identifies a series of concerns with respect to TikTok that include surveillance and intelligence operations, privacy violations, data harvesting, political interference, narrative control and Communist Party of China censorship exports. In that brief, there are also a series of concerns expressed with respect to many other social media companies, such as Snapchat and LinkedIn.

I would be very happy to share this brief with the committee, if you wish to have it.

Mr. Matthew Green: Yes, that would be very helpful.

In your opinion, does the risk of having social media apps on federal government phones differ from that of employees having the same apps on their personal phones?

Mr. Matt Malone: With respect to the type of information being shared on government-issued devices, it would seem unquestionable that there's probably greater sensitivity, especially when this information.... Even if it's harmless on an individual level, it could potentially be useful in the aggregate. You have to think about things like location data, which might reveal things like the location of politicians or members of the Canadian Armed Forces. There was a story a few years ago, from public reporting, about how a leak of location data from a Fitbit-style company led to an ability to map, essentially, an American military base in Helmand province. This data is, obviously, very sensitive in the aggregate.

If you permit, I would go beyond this and say there should be a ban on social media applications on government-issued devices, unless there's a strong business justification.

However, there's also a very strong indication of what the priorities of government are. Earlier, I talked about a lack of funds for the RCMP's cybercrime investigative team. However, if you look at the arsenal of folks who work for the government in social media or communications, it's exponentially larger than the resources and personnel we're devoting to fighting online harms as they are actually experienced by some of the most vulnerable Canadians.

● (1740)

Mr. Matthew Green: I think you even referenced that it was your opinion that we should stop advertising on these platforms. When you look at the risks and the rewards in terms of engagement and getting information out there, it's your position here today that the government should stop. Would that include all platforms?

Mr. Matt Malone: Yes. I believe it's unethical to advertise with social media companies if we have real concerns about data harvesting and illicit foreign interference.

Last year, the government spent a record $141 million on advertising, which was more than twice what the government spent on the administration of the Access to Information Act, and that included almost $2 million on TikTok.

It's really difficult to attend a committee hearing where there are all these concerns about TikTok's practices but then see the government throw money at TikTok, which, in my view, is an implicit endorsement of those practices that we're seeking to critique. I do believe, just to clarify and to make this point clear, that this concern applies to all social media companies.

I was very pleased that the government stopped advertising on Meta over the summer, but that was in retaliation for Meta's conduct with the Online News Act, so that was a bit of a different measure, but even as retaliatory, I support it.

Mr. Matthew Green: That's correct.

I need to go back to Mr. Andrey and Mr. Masoodi.

Has your organization conducted any specific research regarding the sharing of data between social media platforms such as TikTok and foreign entities, whether state actors, private sector or third party, that reuse their data for profiling, marketing and harmful purposes?

Mr. Sam Andrey: Thanks for the question, and thanks for the shout-out to Christelle, who is a wonderful member of our team, as well. I hope she is invited one day to this committee or to INDU on AI.

To answer your question, yes. Joe and I and another colleague, Yuan, wrote a paper that looked at the data storage practices in cross-border data transfers of social media platforms, which is called “Home Ice Advantage”, and we appreciated the shout-out to that report a few meetings ago, as well.

Joe, I don't know if you want to jump in here.

The question even came up a few rounds ago, about TikTok saying it stores its data in Singapore and the U.S. Yes, that's true, but that is an incomplete picture. There can still be remote access to those servers from any country in the world.

Mr. Matthew Green: Since I'm out of time, could you send us any highlights? It was referenced, but any specific highlights and concerns that you submit to this committee can be used as testimony.

Thank you.

The Chair: Thank you, Mr. Green and Mr. Andrey.

Anything our witnesses have been asked to provide in writing, can you do that by this Friday, please? That would help the analysts. We have to put a timeline on it, so Friday at five o'clock, if you don't mind.

We have Mr. Barrett, and then Mr. Kelloway, Mr. Bains, Monsieur Villemure and Mr. Green, who will bring us home. You each have two and a half minutes.

Go ahead, Mr. Barrett.

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Thanks very much, Chair.

We have just a couple of quick minutes.

I want to hear just quickly from each of the witnesses, if I could. Do you see merit in requiring app stores, like the Google Play store and the Apple App Store, to require parental consent for downloading social media apps for children? My question for previous witnesses was for children under the age of 16, so I'll frame it the same way for each of you.

Mr. Sam Andrey: I can start.

I certainly don't think it would be harmful, but I think the logistics around age verification are tricky. I probably don't have time to get into all that right now, but I think, in principle, yes.

I might even suggest going further, since we're talking about trans-border data storage, which is to say that you could ban the transfer of minors' data to countries with insufficient equivalent protection, if you wanted to, as well.

Yes, I think that would be a fine thing to add.

● (1745)

Mr. Michael Barrett: Thanks.

Mr. Malone, go ahead.

Mr. Matt Malone: I would not support that.

I understand the intent behind the proposal. I think it's well-intentioned, and I considered it seriously, but I think it would have adverse effects that may not be what is intended.

The reality is that we need a privacy law that protects children by default. It shouldn't be the responsibility of a parent. There are mixed harms and benefits with these technologies, and I don't believe that parents or older generations are the ones who are always the best at navigating these technologies. I've seen lots of surveys from within the Privy Council Office itself that show young people are the ones who use these technologies; 30% of teens get their news from TikTok, and a lot of older generations don't use them at all. One concern I would have is that I wouldn't feel comfortable entrusting that responsibility to all parents, but that's just my personal view.

What I would say, though, is that I do believe children should be explicitly referenced as a vulnerable population within Bill C-27. I think it's unacceptable that children and youth, in particular, have been removed from Bill C-27 and are omitted. That was a deliberate intent by the Ministry of Industry. I have an internal brief that talks about the reasons behind that, and I'd be happy to share that with you.

The Chair: Thank you, Mr. Malone.

I'm sorry, but we don't have time. If you can do that by Friday at five, we'd appreciate that.

Mr. Bains, you have two and a half minutes. Go ahead, sir.

Mr. Parm Bains (Steveston—Richmond East, Lib.): Thank you, Mr. Chair.

Thank you to our witnesses for joining us today.

It's clear we have a generational risk or danger with online harms. Two tragedies have hit close to home for us in British Columbia. You may recall Amanda Todd's suicide in 2012, which was linked to online harassment, and the recent news of the 12-year-old boy whose suicide was linked to online sexual extortion.

Coincidentally, I have a 15-year-old daughter and a 12-year-old boy, so it's chilling to hear some of these stories that come out.

I'll go to Mr. Malone first.

You've noted in a previous interview that the collection of vast amounts of data creates “power imbalances” with users. Could you please expand on what you mean by that?

Mr. Matt Malone: I provided an answer to the MP for Mississauga—Erin Mills, but I'm happy to extrapolate a little bit on this, particularly in the context of Chinese influence and control.

There have been declarations that.... I'll use TikTok as an example, although the comments would apply to other entities, too. TikTok collects Canadian user data and stores it in the United States, Singapore and Malaysia. According to Chinese law, specifically the National Intelligence Law, there are requirements that companies operating in China co-operate with China. That's specifically article 7 of the law I just referenced. Article 10 of that law provides for extraterritorial application of that law. It wouldn't matter if the data is residing in a foreign jurisdiction. A company that has a base in China, which it does...and the Chinese state holds a 1% share, which allows control over TikTok and ByteDance.

It means that these problems aren't going to go away.

Mr. Parm Bains: You mentioned several platforms earlier, like Bumble and others like that. What about messaging platforms like Signal, Telegram or WhatsApp?

We've seen a recent warning put out by Abbotsford police about WhatsApp phone calls that were made from outside Canada extorting local businesses—

The Chair: Mr. Bains, you're over your time, but I do want to hear the response.

I don't know whom you're directing it to, but could we get a quick response, please?

Mr. Parm Bains: I'll direct that to Mr. Malone again, please.

Mr. Matt Malone: I believe the reasons that folks are using Signal to evade law enforcement are the same reasons that ministers and political staffers are using Signal to avoid the Access to Information Act.

I think all of these social media companies should be banned on government-issued devices.

● (1750)

The Chair: Well, that was an answer.

I appreciate that, Mr. Malone.

[*Translation*]

Mr. Villemure, you may go ahead for two and a half minutes.

Mr. René Villemure: Mr. Malone, at the end of the day, what we are trying to do here is fight surveillance capitalism, data being its bread and butter.

How do we fight surveillance capitalism?

[*English*]

Mr. Matt Malone: I would say that it's important to show, not tell. You need privacy and data protection laws that show Canadians you take privacy and data protection seriously. This means that government conduct must be covered by robust and updated legislation. It also means that political parties, which are often very eager to call out the privacy harms perpetuated by private social media companies, must be covered by Canadian privacy legislation as well.

A lot of young people who would be listening to these thrilling discussions about privacy and data protection in Canada—data harvesting, illicit interference and all of that stuff—would probably come back at you with very different values because they're the ones who actually use these services. A lot of the demographic of lawmakers and members of the executive are the folks who are specifically not using them.

I think it's really hard to build credibility with young people that these issues—and surveillance capitalism in particular—are being taken seriously unless you make these laws applicable to government conduct and the conduct of political parties.

[*Translation*]

Mr. René Villemure: Thank you very much.

The Chair: Are you done, Mr. Villemure? You have some time left.

Mr. René Villemure: I have time left? I don't have my timer to keep track.

The Chair: All right.

[*English*]

Mr. Green, you have two and a half minutes. Go ahead, please.

Mr. Matthew Green: Thank you very much.

Mr. Andrey and Mr. Masoodi, I'm going to provide you the opportunity over the next minute to provide—

[*Translation*]

The Chair: Is everything fine on your end, Mr. Villemure? Do you want to keep going for 30 seconds?

Mr. René Villemure: I'm having technical issues.

The Chair: Very well.

Mr. Villemure is having technical issues. Sorry.

[*English*]

Mr. Green, I'm sorry. Go ahead, sir, for two and a half minutes.

Mr. Matthew Green: I want to give all the witnesses the opportunity, within 30 to 45 seconds or a minute each, to share anything that they want to discuss or highlight that wasn't asked. Obviously, these interventions are directed by our line of questioning.

I'll begin with you, Mr. Andrey or Mr. Masoodi, if you want to share for a minute what you want us to leave with here today.

Mr. Joe Masoodi: Thank you for the question.

There was a question on surveillance capitalism, which is a concept that was introduced by Shoshana Zuboff. It was introduced a couple of times during the hearings. The previous question was on what we can do to try to at least mitigate the impacts of surveillance capitalism, which was really initiated, if we look back, by Google. It was Google, through its machine-learning techniques, that facilitated that process. It was the inadequate regulatory and legal regimes that were in place that allowed that to happen.

If I were to provide some key recommendations or suggestions in terms of takeaways, I would say we need robust privacy laws. We've heard that over and over again. I'd like to emphasize that again. We need to have robust privacy measures in place, specifically in areas with regard to cross-border data transfers. I think Bill C-27 could use an area that specifically identifies cross-border data transfers as an area for robust protections.

Mr. Matthew Green: Okay. I'm now going to go over to Mr. Malone.

Mr. Malone, you have the close-out here. Is there anything at all, for the good and welfare of this committee, that you think might have been missed?

Mr. Matt Malone: My understanding is that folks are very concerned about back doors that China might potentially have to get the type of data that's being collected by TikTok and the opportunities for China to operate as a threat actor that those would provide.

I would say that Canada needs to show rather than tell in this area. By that I mean that we need to hold our own government to account to make sure that it is transparent and accountable and that it protects human rights and democracy online.

You earlier had the Communications Security Establishment and the head of CCCS speak at this committee on this study. CSE will neither confirm nor deny that it's using spyware against foreign adversaries as part of its work. You're not going to get an answer about whether China is doing that when Canadian authorities won't provide a clear answer either.

I would also just say that I would really like to see whatever information CSE gave to PCO or TBS in the lead-up to banning TikTok, because it's really strange that this social media app was selectively banned. The timing is notable, because it was obviously 10 days after an explosive report came out.

● (1755)

Mr. Matthew Green: In your opinion, was it a political decision?

Mr. Matt Malone: I have no opinion.

[*Translation*]

The Chair: Mr. Villemure, you're not frozen anymore. Do you want your 30 seconds to ask another question?

Mr. René Villemure: Yes, please.

Please continue, Mr. Malone.

[*English*]

Mr. Matt Malone: I don't have anything else to say.

[*Translation*]

The Chair: Thank you, Mr. Villemure.

[*English*]

First of all, I want to thank all of our witnesses—Mr. Malone, Mr. Andrey, and Mr. Masoodi—for being here today.

If you have any written documents you'd like to provide to the clerk and the committee, please do so by Friday at 5 p.m. You've provided some pretty valuable information today, and I really appreciate it. I also appreciate your patience as we went through votes, and your patience for coming back this week.

I'm going to dismiss the witnesses, as I have a couple of things for the committee. It's just an update.

I am in receipt of an emergency meeting request. We are going to do that on Wednesday. The notice should be out shortly.

I will tell you, as well, that we have received confirmation from Google and Meta that they will appear before the committee as part of this study on Wednesday, December 13. We will have both those entities here next week.

There being no other business, I am going to adjourn the meeting.

Thank you all for being here. Thank you to our analysts, our clerk, and our technicians.

The meeting is adjourned.