HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

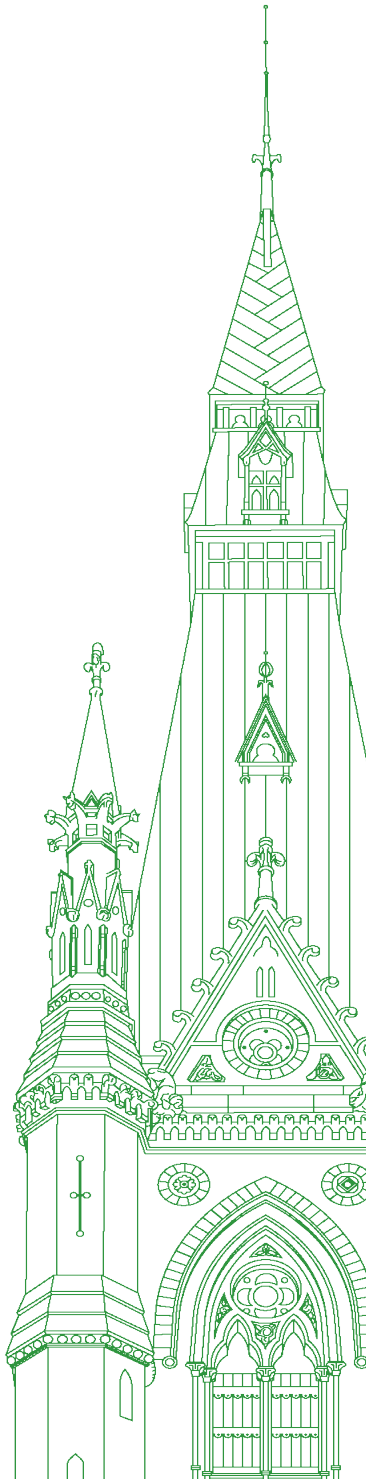
Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 097

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Wednesday, December 13, 2023



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Wednesday, December 13, 2023

● (1640)

[*English*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): Good afternoon, everyone.

I apologize for the late start, but I do call the meeting to order.

Welcome to meeting number 97 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[*Translation*]

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.

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'd like to remind all members not to put earpieces near the microphones, for obvious reasons. It does cause feedback and potential injury.

I'd now like to welcome our guests and witnesses today. All have the proper equipment and connection. We've done all the technical tests, and yes, things seem to be working properly.

We have a full slate today, and I want to welcome you all.

From Google Canada, we have Jeanette Patell, head of Canada government affairs and public policy, YouTube; and Shane Huntley, senior director, threat analysis group. From Meta Platforms, we have Rachel Curran, head of public policy, Canada; Nathaniel Gleicher, head of security policy; and Dr. Lindsay Hundley, influence operations policy lead. From X Corporation, I want to welcome Wifredo Fernández, head of government affairs, United States of America and Canada; and Josh Harris, senior privacy and data protection counsel.

We are going to start with Google.

You have up to five minutes for your opening statement to the committee. Go ahead, please.

[*Translation*]

Ms. Jeanette Patell (Head of Canada Government Affairs and Public Policy, Google and YouTube, Google Canada): Mr. Chair, ladies and gentlemen of the committee, good morning.

My name is Jeanette Patell. I am responsible for government affairs and public policy for Google and YouTube in Canada.

[*English*]

I am joined by my colleague Shane Huntley, who leads a group dedicated to protecting Google and its users from advanced threats, including those posed by state-sponsored attacks.

[*Translation*]

We recognize the committee's efforts to make Canadians aware of the unethical and illegal harvesting and sharing of personal data and the risks to which Internet users around the world are exposed.

[*English*]

Data plays an important role in making the products and services that Canadians use each day more helpful. When Canadians use our services, they are trusting us with their information. This is a responsibility that we take very seriously at Google. We protect user privacy with industry-leading security infrastructure, responsible data practices and easy-to-use privacy tools that put our users in control.

Tools such as our privacy checkup and our security checkup give people personalized privacy and security reminders and recommendations, including flagging actions that they should take to immediately secure their Google account.

[*Translation*]

These two verification functions allow users to customize, step by step, the security and confidentiality controls based on their personal preferences.

[*English*]

We also have an advanced protection program, which is available to anyone but is specifically designed for individuals and organizations—such as elected officials, political campaigns, human rights activists, and journalists—who are at a higher risk of targeted online attacks.

Treating our user data responsibly and protecting user privacy include protecting data from third parties. That's why it's our strict policy to never sell our users' personal information to anyone. When it comes to government requests for user information, our team carefully reviews each request to make sure that it satisfies applicable laws. If a request asks for too much information, we try to narrow it, and in some cases, we object to producing any information at all. We have also taken the lead, through our transparency reports, in being transparent about government requests for user information.

In addition to these industry-leading tools and strict protocols, we invest significantly in global teams and operations to prevent abuse on our platforms. One of those teams is our threat analysis group.

I'll now let my colleague Shane speak about the work that his group does to secure our users' information against bad actors.

Mr. Shane Huntley (Senior Director, Threat Analysis Group, Google, Google Canada): Thank you, Chair and members of the committee.

As Jeanette mentioned, I'm the director of Google's threat analysis group, or TAG. While I'm personally based in Australia, we are a global team, a significant part of which is based in Google's Montreal office, which I'm sure this committee well knows is a growing hub of cybersecurity talent and expertise.

Our global team of analysts and security experts works closely with product teams to analyze and counter threats to our platform and our users, including threats from government-backed attackers, serious cybercriminals and information operations.

Hostile actors continue to attempt to access and misuse our platforms, and Google has invested heavily over many years to counter attempts to deceive, harm or take advantage of users. We don't just mitigate security risks; we work to eliminate entire classes of threats for consumers and businesses whose work and lives depend on the Internet.

On any given day, TAG tracks more than 270 targeted or government-backed attacker groups from more than 50 countries. We publish a quarterly bulletin about actions we take against accounts that we attribute to coordinated influence campaigns. For instance, in the third quarter of 2023, we reported disabling influence campaigns originating from groups including Russia, Iran, China and Mexico.

We are particularly focused on disrupting coordinated influence operations on YouTube. For example, since January 2023, we terminated more than 2,400 YouTube channels linked to Russia and more than 60,000 channels linked to China as part of our investigations into this activity. These actions are in addition to YouTube's ongoing enforcement of community guidelines, which resulted in the removal of more than eight million videos globally in the third quarter of 2023.

As we discover and disrupt operations, we take steps to protect users, disclose information publicly and share our findings with industry and government partners to support the entire ecosystem. We also issue warnings to our users when we believe that they have been targeted by a government-backed attack.

While this work is never done, we continue to take action, identify bad actors and share relevant information to protect users and prevent future attacks.

We would like to thank the committee for your attention to this critical issue and for allowing us to share more on our work to keep Canadians safe and our investments in the right expertise to protect users on our platform. We remain committed to partnering with the Canadian government to ensure a stronger and safer digital future for all Canadians.

We look forward to answering your questions.

● (1645)

The Chair: Thank you, Mr. Huntley and Ms. Patell.

We're going to go to Meta now.

You have five minutes to address the committee. Please go ahead.

Mr. Nathaniel Gleicher (Head of Security Policy, Meta Platforms Inc.): Thank you for the opportunity to appear before you today.

My name is Nathaniel Gleicher, and I'm the head of security policy at Meta.

My work is focused on addressing the adversarial threats that we face every day to the security and integrity of our products and services and taking steps to protect our users in every way we can.

I have worked in cybersecurity and trust and safety for two decades, first as a technical expert and then as a cybercrime prosecutor at the U.S. Department of Justice and as director for cybersecurity policy at the National Security Council.

I'm joined by video conference today by two colleagues at Meta: Rachel Curran, the head of public policy for Canada; and Dr. Lindsay Hundley, our lead for influence operations policy.

At Meta, we work hard to identify and counter foreign adversarial threats, including hacking campaigns and cyber-espionage operations, as well as influence operations, what we call coordinated inauthentic behaviour, or CIB, which we define as any “coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation.”

CIB is when users coordinate with one another and use fake accounts to mislead others about who they are and what they are doing. At Meta, our community standards prohibit inauthentic behaviour, including by users who seek to misrepresent themselves, use fake accounts or artificially boost the popularity of content. This policy is intended to protect the security of user accounts and our services and to create a space where people can trust the people and communities they interact with on our platforms.

We also know that threat actors are working to interfere with and manipulate public debate, exploit societal divisions, promote fraud, influence elections and target authentic social engagement across the Internet. Stopping these bad actors, both on our platforms and more broadly, is one of our highest priorities. That's why we have invested significantly in people and technology to combat inauthentic behaviour.

The security teams at Meta have developed policies, automated detection tools and enforcement frameworks to tackle deceptive actors, both foreign and domestic. These investments in technology have enabled us to stop millions of attempts to create fake accounts every day and to detect and remove millions more, often within minutes of their creation. Just this year, Meta has disabled almost two billion fake accounts. The vast majority of those, more than 99% of them, were identified proactively before receiving any report.

As part of this work, we regularly publish reports on our work to counter the threats we're discussing here today. To talk more about that, I'd like to hand it over to Dr. Hundley, who coordinates our work to identify and expose foreign interference.

Dr. Lindsay Hundley (Influence Operations Policy Lead, Meta Platforms Inc.): My name is Lindsay Hundley and I lead Meta's policy work on countering influence operations, both overt and covert. My work at the company draws on my nearly 10 years of experience as a researcher focused on issues related to foreign interference, including in my doctoral work at Stanford University and during research fellowships at both Stanford and Harvard.

Meta uses a behaviour-based approach to identify covert influence operations, not one that's based on the content they share. We remove networks like these no matter who is behind them, what they post, or whether they are foreign or domestic. If helpful, I would be happy to give specific examples.

We have taken down more than 200 covert influence operations from 68 countries in at least 42 languages from Amharic and Urdu to Russian and Chinese. We regularly report these findings through our adversarial threat reports. Sharing this information has enabled our teams, investigative journalists, government officials, and industry peers to better understand and expose Internet-wide security risks, including ahead of critical elections.

As of our latest report, China is now the third most common geographic source of foreign CIB that we have disrupted, after Russia and Iran. This year, we have taken down five CIB networks from China, more than any other country. Regardless of who was behind these networks, or what they targeted, these CIB operations emanating from China typically posted content related to China's interest in different regions worldwide. Many praised China. Some defended its human rights records in Tibet and Xinjiang. Others criticized critics of the Chinese government, including journalists and researchers.

Countering foreign influence operations is a whole-of-society effort. No single platform can solve foreign interference on its own, which is why we work with our industry peers, independent researchers, investigative journalists, government and law enforcement.

Thank you for your focus on this work. We look forward to answering your questions.

● (1650)

The Chair: Thank you, Dr. Hundley. That was precisely on time between the two of you. Thank you for that.

Now we're going to go to X Corporation.

Please go ahead, for five minutes, to address the committee.

Mr. Wifredo Fernández (Head of Government Affairs, United States of America and Canada, X Corporation): Mr. Chair and members of the committee, thank you for the invitation to appear before you today.

My name is Wifredo Fernández. I serve as head of government affairs for the U.S. and Canada at X. I'm joined by my colleague Josh Harris, our lead privacy counsel for North America.

X's mission is to promote and protect the public conversation and to be the town square of the Internet. People's right to privacy and data protection is a fundamental right, not a privilege. X is a uniquely open service. We offer a range of ways for people to be a part of the conversation on X on their terms, from creating pseudonymous accounts in order to protect their identity to letting people control who sees their posts.

Our privacy efforts have enabled people around the world using X to protect their own data. That same philosophy guides how we work to protect the data people share with us. We empower people who use our service to make informed decisions about the data they share with us. We believe individuals should know and have meaningful control over what data is being collected about them, how it's used and when it's shared. We're guided by the principle that we should only use data for the purpose for which it was collected.

We have one global privacy program that encompasses the highest data protection standards in the world, and a single global privacy policy, which we have worked hard to make clear and easy to understand. X is always working to improve transparency into what data is collected and how it is used. Through the account settings on X, we give people the ability to make a variety of choices about their data privacy, including limiting the data we collect, determining whether they see interest-based advertising, and controlling how we personalize their experience. In addition, we provide people with the ability to access information about advertisers that have included them in tailored audiences to serve them ads, demographic and interest data about their accounts from ad partners, and information X has inferred about them.

Behind the scenes, teams across the company are constantly working to protect the privacy and data of those who use our service. This work has several areas of focus. Over the last year, we have been overhauling technical infrastructure and products to make X more efficient and durable. Tackling technical debt isn't just good for the privacy and safety of people who use X. It will also help us get better products and services to people faster.

Privacy by design is a priority with every product we build. We execute comprehensive privacy reviews for all new features and tools we roll out, and perform additional data protection impact assessments for products that may pose additional risks to our users.

In addition, we have taken steps to mitigate unauthorized scraping and harvesting of X data. No single mitigation can protect against all the privacy harms associated with such activity. Some actions we've taken include the use of dedicated teams that work together to monitor, identify and mitigate scraping activity across a range of vectors and platforms; the introduction of rate limits to limit a malicious actor's ability to scrape data; the expansion of user verification offerings to assess whether a given account applicant is a real person, not a bot; and updates to our terms of service, in order to make it clear that scraping is an express misuse of the X service.

X is public. Posts are immediately viewable and searchable by anyone around the world. We give people non-public ways to communicate on X, too, through protected accounts and direct messages. It is also possible to use X under a pseudonym, if you prefer not to use your real name. When people use X, even if they're just looking at posts, we receive some personal information, such as the type of device they're using and their IP address. People can choose what additional information to share with us, including email address, phone number, address book contacts and a public profile. We use the information for things such as keeping accounts secure and showing people more relevant posts to follow—events and ads.

Like many peer companies, X's business is largely based on advertising, but we have some fundamental differences. In general, rather than focusing on who you are, our data is more about what you're interested in—for example, what you repost, what you like and whom you follow, all of which is public. X has an open public API, making data available for developers, journalists, brands and researchers for analysis, and to build businesses, provide services and create innovative products. We do not provide personally identifiable information through our API that is not already visible on the service. We take our responsibility to protect people's data seriously and have strict policies and processes in place to assess applications for uses of X data and restrict improper use of such.

Notwithstanding the fact that our API only makes available public data, we have long-standing rules against the use of our data for surveillance. As a company, we will always err on the side of protecting the voices of those who use our service. Privacy and data protection are at the heart of our company-wide priority to build products that earn the trust of people who use them. Freedom of speech and expression is built on this foundation, and we take this responsibility very seriously.

Thank you, and we look forward to answering your questions.

● (1655)

The Chair: Thank you, Mr. Fernández.

Thank you, all, for your opening statements.

Members of the committee, we have a bit of a Brady Bunch scenario going on here.

Mr. Green, I'll call you “Mike Brady”, the patriarch of the family.

I'm going to ask that members direct their questions specifically to an individual, because we're just going to waste time trying to figure out who's going to answer the question. If you can do that, it would be appreciated.

We're going to start our first six-minute round with Mr. Barrett from the Conservative Party.

Mr. Barrett, go ahead, please.

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): I'll direct my first question to X Corporation.

Would you support an age restriction requiring parental approval for downloads of your app by children under the age of 16?

Mr. Wifredo Fernández: Thank you for the question.

There are, around the world, a variety of different laws when it comes to consent and age restrictions. Sometimes they vary by state here in the United States. We welcome the opportunity to engage on any potential legislation—

Mr. Michael Barrett: I'm sorry. I'm just going to jump in there quickly, sir.

This is a great opportunity for you to engage on whether X Corporation would support a restriction in the App Store for minors under the age of 16 to require parental consent when they're downloading your app. Would you support that?

Mr. Wifredo Fernández: As you may imagine, X is not the platform of choice for teens. We do allow, in the United States and Canada—with the exception of Quebec, which is over 14—the ability to use the service. We leave the decision of whether to restrict on the App Store to the App Store.

Mr. Michael Barrett: Okay.

I have the same question for Meta, please.

Ms. Rachel Curran (Head of Public Policy, Canada, Meta Platforms Inc.): Thank you, Mr. Barrett.

Yes, we would support that kind of restriction. If I may say, I think that would be an excellent way for policy-makers to protect and address youth safety issues, as long as it's applied industry-wide.

Mr. Michael Barrett: Thank you for your response.

I have the same question for Google, please.

Ms. Jeanette Patell: You can put parental controls on an Android device. That's one of the things we've built in order to put families and caregivers in control of [*Technical difficulty—Editor*] experience.

That can restrict what content can be downloaded or purchased from Google Play on that particular device, based on the maturity [*Technical difficulty—Editor*] level and concerns in putting this [*Technical difficulty—Editor*] that is right for them.

The Chair: I'm sorry, Ms. Patell. The interpreters are having a problem because you are cutting in and out.

Mr. Barrett, I'm going to stop your time here.

I don't know.... We did the test, and it was fine.

I'm going to go back to Mr. Barrett here, but we may have a problem, Ms. Patell. We'll see what the next answer brings.

Go ahead.

Mr. Michael Barrett: Okay, Ms. Patell. I heard your response that on Android Google devices parents have the opportunity to set content moderation by age. Can you indicate if that's a correct summary of what you said?

Ms. Jeanette Patell: Essentially, yes. We have built tools so that parents can put controls on the devices and downloads for [*Technical difficulty—Editor*].

Mr. Michael Barrett: Thanks very much.

My next question is for X Corp.

Do you have a list of instances in which the Government of Canada has requested that content be taken down on your platform? That's by the Government of Canada to X Corp.

● (1700)

Mr. Wifredo Fernández: I'll allow my colleague Josh to add to this.

We do keep track of lawful requests for user information from governments. We don't have that information in front of us today, but yes, law enforcement do have a particular portal where they can make lawful requests for user data or potential content removal, according to lawful order.

Mr. Michael Barrett: Before your colleague jumps in there—and you can give a response in under 30 seconds—I'm looking for requests by government and not by police agencies.

That's for X, please.

Mr. Josh Harris (Senior Privacy and Data Protection Counsel, X Corporation): Yes, we do track by government agency. We would be able to provide you with aggregate numbers of government requests from Canada for a set period—for example, one year.

Mr. Michael Barrett: If you're able to give us the last five years and table that with the committee, can you also itemize it by the nature of the request, if you're providing a written submission to the committee? Is that something you'd be able to do, sir?

Mr. Josh Harris: Yes. I'll have to explore that with my colleagues to make sure that we'll be able to get that granular enough to be useful to the committee.

Mr. Michael Barrett: Is there a Canadian version of the "Twitter files"?

Mr. Josh Harris: Not to my knowledge.

Mr. Michael Barrett: I have the same question for Meta with respect to takedown requests by the government.

Is that something that you keep track of, and if so, are you able to itemize the frequency and the nature of each occurrence? Is that something you would be able to provide to the committee in writing, Ms. Curran?

Ms. Rachel Curran: Yes, we can. We respond to valid government requests in accordance with applicable law and our terms of service. Those requests are publicly disclosed at our transparency centre, and we'd be happy to provide more detail on those to the committee.

Mr. Michael Barrett: Just very quickly, because I only have 15 seconds left, Ms. Patell, is that something that Google would be able to do?

Ms. Jeanette Patell: Yes, absolutely. We publish every six months a transparency report with government removal requests, and we'd be happy to provide that information to the committee.

Mr. Michael Barrett: Thank you very much.

I have about 10 seconds left.

Chair, I hope we're going to have the opportunity for another round of questions with Ms. Vecchio. She wants to look into the protection of minors from exposure to sexually explicit material online, particularly, I would say, including links to the online crime scene that is Pornhub. That's just a flag for all of you to expect some questions about that in the next round from us.

The Chair: Thank you, Mr. Barrett, for that. That concludes your round of questioning.

I am going to just make it clear that if a written response is required because of a request from the committee, we will have the clerk follow up with each one of you on what that specific request is to provide documents. Then we're going to set a deadline for a week from today for those documents to be provided to the committee. That's just to make it clear for everyone.

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

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

Thank you to the witnesses for appearing and for your presentations. I appreciate that all of you talked about foreign interference and the protection of Canadian data. It's incumbent upon all of us to be proactive about the protection of Canadians.

I will turn to Meta first.

There was a $9-million penalty in 2020 in Canada for misleading privacy claims, a $5-billion penalty for deceiving users in the U.S., and a 405-million-euro penalty in 2022 in Europe. There are a lot more sanctions. What is the issue here with respect to protecting Canadians' privacy here in Canada?

Ms. Rachel Curran: I assume you're talking about Cambridge Analytica, which was some years ago now. As we've always maintained, there was no evidence that Canadians' information was shared with Cambridge Analytica. Meta also does not sell our user data, at all, unequivocally. Indeed, even when the Federal Court examined the Cambridge Analytica issue, they agreed with our position, finding that there was insufficient evidence that Canadians' data was shared and that, in any event, Facebook's data-sharing practices were adequately disclosed.

That said, in the last few years, certainly since 2019, we have transformed privacy at Meta and built one of the most comprehensive privacy programs in the world. We look forward to building products and services that people love, trust, and use with privacy at the forefront.

● (1705)

Ms. Iqra Khalid: Thank you.

Where do you store Canadian data?

Ms. Rachel Curran: I don't know the answer to that.

Ms. Iqra Khalid: Can we get an answer to that, please, if that's okay?

Ms. Rachel Curran: I will commit to getting back to the committee.

Ms. Iqra Khalid: Thank you very much.

To Google, how do you make money on people's personal data?

Ms. Jeanette Patell: Thank you for the question and the opportunity to share more about our practices.

We build products and services that are secure by default and private by design. As we make publicly clear, a majority of our revenue is built upon advertising. Our commitment to our users is to give them visibility into how their information is informing their experience on our services, to give them tools for transparency and to ultimately put them in control in how their information is being used.

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

I looked at the Apple App Store earlier. Chrome, which is a product of yours, links location, audio data, search history, browsing history, identifiers, usage data, and then “other data” to individuals. What do you do with all that information? How do you use that?

Ms. Jeanette Patell: Information ultimately helps make our products function properly and effectively, makes them more secure, gives the ability to detect and mitigate fraud, and makes them more helpful for individuals. We provide settings for individuals to make the choices that are right for them in terms of how their information is being collected and used.

We have something called the privacy checkup centre, as well as a My Ad Center, where individuals can see at a pretty granular level how this information is being used to inform their experience with our services. They have the opportunity to either delete that information or turn off things like personalized advertising.

Ms. Iqra Khalid: Does it actually get deleted?

Ms. Jeanette Patell: Yes. I can't go into detail on our data retention policies here, because I'm just not an expert in that domain, but we do provide information to individuals about this in their privacy centre.

We also have been leading in putting in place an auto-delete function for new accounts. Having that function auto-deletes information after 18 months.

Ultimately, this is all about users being able to make the choices that are right for them. That's where transparency and providing settings for everybody are a big part of our commitment to privacy by design.

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

Can you talk to us about tags on YouTube, specifically MGTOW? It stands for “men going their own way”, which is associated with misogyny through male supremacy ideology.

Do you think that allowing such tags impacts the privacy and also the safety of Canadians?

Ms. Jeanette Patell: Maybe I'll take a step back and speak to how we apply our content policies on YouTube.

It's important because our community guidelines, which are quite comprehensive, apply to all content on our platform, whether that's comments, external links or the video itself, etc. Responsibility is really at the core. It underpins our entire platform at YouTube.

When we look at specific instances like this—I'm not a trained reviewer in trust and safety, but we have over 20,000 people trained in this domain—and when we become aware of a concern around that, we would assess whether each piece of content does meet the standards of our community guidelines.

Ms. Iqra Khalid: Do you think—

The Chair: That's it, Ms. Khalid. It was more than six minutes.

Thank you, Ms. Patell.

I want to make sure everyone has their French interpretation on.

● (1710)

[*Translation*]

Mr. Villemure, you have the floor for six minutes.

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

My first questions are for Meta's representative, Ms. Curran.

Ms. Curran, you are Meta's head of public policy in Canada.

Is that correct?

[*English*]

Ms. Rachel Curran: That's correct.

[*Translation*]

Mr. René Villemure: The committee is concerned not only with privacy and the protection of personal information, but also with ethics.

Do you think that the omnipresence of social networks, such as Facebook, in people's daily lives means that they should be considered an essential service?

[*English*]

Ms. Rachel Curran: No, I wouldn't say they're an essential service. I think they are tools and products that Canadians enjoy using. They enjoy using our platforms to share information about their families and friends. They enjoy finding out what's happening in their communities. They're really tools that Canadians use to connect with one another. I think that's particularly important in a country like ours, which is so geographically spread out. Communities are far apart from one another. We're dispersed across a very large territory.

We think Meta's products and services help Canadians connect with one another, not as essential services, but as tools that Canadians enjoy using.

[*Translation*]

Mr. René Villemure: You say that Canadians share information on social media, including news-related content.

Meta has chosen to block local Canadian news on its platform. Do you think this is preventing people from accessing quality information?

[*English*]

Ms. Rachel Curran: Monsieur Villemure, we would love to not be in this position. We would love to have news on our platforms. The problem is that the government, through Bill C-18, the Online News Act, has asked us to pay an uncapped amount, an unknown amount, for content that has no commercial value to us.

We believe we provide a great deal of value to news publishers in the form of free distribution and marketing. That amount we've calculated at $230 million per year. We would love to get back to putting news on our platforms and providing publishers with those free tools. We're not able to do that under the framework of the Online News Act.

Mr. Villemure, if you could work with your government colleagues to make amendments to that legislation that would allow us to put news back on our platforms, we would love to do that.

[*Translation*]

Mr. René Villemure: I agree with you.

The media are the fourth estate. In particular, the media enable citizens to understand what's going on and make informed decisions. Personally, I find it rather troubling that Meta doesn't go one step further. It's a private company, and it has the right to make money, of course.

You say that the government should act. What are you proposing?

What are you proposing so that Canadians and Quebecers can be well informed?

[*English*]

Ms. Rachel Curran: We think, Mr. Villemure, that there is still a lot of credible information on our platforms. There is information from Quebec policy-makers. There is information from civil society in Quebec. There is information from non-governmental organizations that are based in Quebec. All of those outlets, all of those individuals and groups still have a presence on Facebook and Instagram, and they're still able to share information with Quebeckers.

Where the problem is, and where we're stuck, is with respect to news outlets. If we can solve that problem, we could put news content back up on our platforms.

We still think there is a lot of credible information on our platforms for Quebeckers to access.

[*Translation*]

Mr. René Villemure: I represent the riding of Trois-Rivières, where the local media are dying. They're not big media, but small ones. They're closing down one after the other, because they can no longer afford journalists and in-depth reporting.

Of course, the national media are still there. But the local media industry is being killed off. I think the responsibility is at the very least shared.

What are your observations on this subject?

[*English*]

Ms. Rachel Curran: Yes, I think there's a genuine public policy issue to address here, which is, how do we best support local media and journalism? It's a cornerstone of our democracy.

Meta was very involved in supporting media outlets and supporting journalism in Canada. We had private deals that were worth close to $20 million per year with news outlets across the country, including in Quebec. Those are no longer possible under the framework of the Online News Act.

I think we need to figure out, as industry, as policy-makers, how to support journalism and how to support the local news ecosystem in a way that makes sense for all of us. It doesn't make sense to try to extract money from two American tech companies to prop up the Canadian news ecosystem, so let's figure out, together, a better solution.

● (1715)

[*Translation*]

Mr. René Villemure: What can our committee do to bring local media back to Facebook?

[*English*]

Ms. Rachel Curran: I would suggest this, Monsieur Villemure. We have heard this from local publishers as well.

We are a very different platform from Google. We do not scrape news content from the Internet or aggregate it in our search results. It has very little commercial value to Facebook or Instagram.

If we were carved out of the Online News Act, so that the requirements of that act did not apply to us, or if there was a carve-out for local journalism, we could bring that back onto our platforms.

The Chair: Thank you, Ms. Curran.

[*Translation*]

Thank you, Mr. Villemure.

[*English*]

Mr. Green, go ahead for six minutes.

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

Welcome to all the guests who are present.

I'm going to put a series of questions to you in a rather rapid way. If I reclaim my time, it's not to be rude, and I'm certainly not trying to make anything personal, but I'm going to put forward some pretty quick questions.

I'm going to start off with Mr. Fernández.

Mr. Fernández, Amnesty International, in a recent report, cited your shift in the new privacy policy, which allows you to collect users' biometric data and access encrypted messages, but “biometric” is not determined or defined.

How do you define “biometric data”?

Mr. Wifredo Fernández: If I may, I will pass that to my colleague Josh, who is the privacy counsel.

Mr. Josh Harris: In the instance of the biometric data that's referred to in the updated privacy policy, that's speaking specifically to information that might be presented on somebody's identification card. For example, this might be a picture or any other biometric information that might be on that identification card that they would have presented pursuant to their application to—

Mr. Matthew Green: How would it be stored?

Mr. Josh Harris: It would be stored like any of our other information pursuant to our data classification systems. This would be higher sensitivity—

Mr. Matthew Green: Has X ever experienced data breaches?

Mr. Josh Harris: Yes.

Mr. Matthew Green: You're storing biometric information the same way you store other information, and you're a company that has already been a victim of data breaches. Is that correct?

Mr. Josh Harris: No, I didn't say it's the same way that we store other information. We would do it pursuant to our data classification system. The biometric information would be higher sensitivity. Then there would be more restrictions on the storage of that data.

Mr. Matthew Green: Would you agree that this is the highest of sensitive information, and that it poses a pretty significant security and privacy risk?

Mr. Josh Harris: Yes, I would.

Mr. Matthew Green: Also, what are you doing with that information specifically? Can you sell it?

Mr. Josh Harris: No. We're not doing anything with the biometric information that we have, other than to note that it is facial biometric information that is present on ID cards.

Mr. Matthew Green: Are you using that to train any AI systems or any other technology that might be used?

Mr. Josh Harris: No, we're not.

Mr. Matthew Green: Then what's the purpose of collecting it?

Mr. Josh Harris: We'll need that identification, for example, if we need parental consent for somebody to create an X account.

Mr. Matthew Green: On your 500 million users, you're collecting all of this biometric information. When people click on, do you believe that the users in this new privacy statement have informed consent when they're clicking through?

Do they know what it is they're consenting to?

Mr. Josh Harris: Yes, I believe they do. We work very hard to make sure that our privacy policy is as clear as possible.

Mr. Matthew Green: Is it written by your legal department?

Mr. Josh Harris: It's written across a number of teams, including our legal department.

Mr. Matthew Green: Do you believe that the average person has the ability to understand the terms and references of a privacy agreement?

Mr. Josh Harris: Our hope is that we're getting to a place where people can understand those terms.

Mr. Matthew Green: It's your "hope"....

Mr. Josh Harris: I believe that they can.

Mr. Matthew Green: You believe that they do.

Mr. Josh Harris: Yes.

Mr. Matthew Green: You believe that young people, teenagers, people who are posting their driver's licence online, have the ability to understand what it is they are consenting to.

Mr. Josh Harris: Yes.

Mr. Matthew Green: That's your position here in your testimony.

Mr. Josh Harris: Yes, that is the nature of our privacy policy.

Mr. Matthew Green: That's fascinating.

Okay. I'm going to move on to Meta.

According to a New York Times article published on November 25 of this year:

> Meta has received more than 1.1 million reports of users under the age of 13 on its Instagram platform since early 2019 yet it "disabled only a fraction" of those accounts....
>
> Instead, the social media giant "routinely continued to collect" children's personal information, like their locations and email addresses, without parental permission, in violation of a federal children's privacy law....

Ms. Curran, how do you respond to that?

● (1720)

Ms. Rachel Curran: Listen, we think youth safety is a really key priority for us. We've developed over 30 new tools and features to support safe and positive experiences for teens on our platforms.

I'll just run through some of these very quickly.

Mr. Matthew Green: Before you do that, I want you just to consider that in the same article it says:

> The unsealed filing said that Meta "continually failed" to make effective age-checking systems a priority and instead used approaches that enabled users under 13 to lie about their age to set up Instagram accounts. It also accused Meta executives of publicly stating in congressional testimony that the company's age-checking process was effective—

I assume that is what you are about to do in your response.

> —and that the company removed underage accounts when it learned of them—even as the executives knew there were millions of underage users [online].

The article goes on to state:

> An internal company chart displayed in the unsealed material, for example, showed how Meta tracked the percentage of 11- and 12-year-olds who used Instagram daily....

How do you respond to that?

Ms. Rachel Curran: Mr. Green, look, we do our best with age verification and with the tools we have available. We remove accounts that don't meet the age standard when we find out that they are underage.

Listen, I'm not—

Mr. Matthew Green: How about this, Ms. Curran?

The article published by The New York Times on October 24 of this year states:

> ...Meta had "designed psychologically manipulative product features to induce young users' compulsive and extended use" of platforms like Instagram. The company's algorithms were designed to push children and teenagers into rabbit holes of toxic and harmful content, the states said, with features like "infinite scroll" and persistent alerts used to hook young users. The attorneys general also charged Meta with violating a federal children's online privacy law, accusing it of unlawfully collecting "the personal data of its youngest users" without [parental consent].

The Chair: Mr. Green—

Ms. Rachel Curran: We disagree with that, Mr. Green.

Look, mental health is a complex, individualized issue impacted by a variety of societal and emotional factors. As—

The Chair: Thank you, Ms. Curran.

Ms. Rachel Curran: —many experts in the field say, it's wrong and even irresponsible to suggest that a single factor is the cause of trends in teen mental health—

The Chair: Ms. Curran, I apologize. We are over time by a bit here.

That concludes our first round. If there are any other issues that you want to address, perhaps you can do that in the next round.

We have Mrs. Vecchio for five minutes.

Go ahead, please.

Mrs. Karen Vecchio (Elgin—Middlesex—London, CPC): Thank you very much.

Today in the House of Commons, we actually passed Bill S-210 to go to committee. It's looking at age verification to ensure that minors are not seeing pornography.

I'm going to start with you, Jeannette, if you don't mind, regarding parental controls. Can you share with me right now how many children, as you're investigating, are able to bypass those parental controls? Do you have statistics showing that?

Ms. Jeanette Patell: Maybe what I can speak to is the fact that YouTube, for example, as you are likely aware, is designed for users 13 years of age and older. In order to have a YouTube account, they have to go through a process where date of birth is provided. Our system—

Mrs. Karen Vecchio: I have a quick question on that. My son, who's 20 years old, is probably celebrating his "40th" birthday soon. Can you not just lie about your date of birth?

Ms. Jeanette Patell: Let me walk you through the steps. We have a neutral process where we ask for a date of birth. If a user indicates that they are under the age requirement, for example, there are no take-backs. That attempt is blocked. We funnel them through to our parental supervision process.

That said, if our system does—

Mrs. Karen Vecchio: Okay. I appreciate that. Very quickly, because I don't have a lot of time, what does that look like? At what point do you find out? Specifically with pornography, if you were going to go and rent a movie, you would have to be over the age of 18. If you're able to get pornography online, how can we ensure that children under the age of 18 are not able to get pornography?

● (1725)

Ms. Jeanette Patell: Maybe I'll speak to two things here.

First, pornography is not allowed on YouTube. Any sexually explicit content or nudity is not allowed on YouTube. That violates our community guidelines. For—

Mrs. Karen Vecchio: I have a quick question there. You've noted how many times...and I've seen that people are pulling down accounts. Have you had to pull down pornography from your regular YouTube sites?

Ms. Jeanette Patell: We publish quarterly transparency reports. We break down the reasons for which we would be removing any content. Yes, we would be removing sexually explicit content or content where there is nudity. That would be one of the areas where we are enforcing our policies.

I think it's important to note that over 90% of the time, that violative content is first detected by our machines. That allows us to deal with this at scale and to do it rapidly. We can remove content rapidly from our systems. We also enable users to report content they have concerns around so that it can be reviewed and removed if it violates our policies.

Mrs. Karen Vecchio: That's very fair. I appreciate that.

Maybe I can move over to Facebook and talk about that. We were talking about rabbit holes, where 11- and 12-year-olds are getting into rabbit holes. I think that's what led me to finding pornography one time, unintentionally, with my 11-year-old son.

Perhaps you could share with me what there is in Facebook to ensure that there is nothing online that is explicit and that a child or an adult who does not intend to would be able to access, to ensure that we don't go down some type of rabbit hole like that.

Ms. Rachel Curran: Thank you for raising this really important issue, Mrs. Vecchio.

Facebook significantly restricts the display of nudity or sexual activity on our platforms. We don't allow it. In fact, we remove sexual imagery to prevent the sharing of non-consensual or underage content as well. Restrictions on the display of sexual activity also apply to digitally created content unless it's posted for educational or satirical purposes. We remove any explicit material.

In fact, we've previously run into criticism for over-enforcing on that kind of material and not allowing images of breast feeding, for instance. We're constantly working to make sure our policies are nuanced enough so that we're not over-enforcing on explicit imagery.

Mrs. Karen Vecchio: Perfect. Thank you so much.

I'm going to switch over to X Corporation. When it comes to explicit content, again, we know that rabbit holes are there. What do you do to ensure that explicit content is not available to the viewers?

Mr. Wifredo Fernández: Users who are under 18 or who did not include a birthdate on their profile are restricted from viewing such content.

The Chair: Thank you, Mrs. Vecchio.

Mr. Bains, you have five minutes. Go ahead, sir.

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

Thank you to our witnesses for joining us today.

I'll begin my first question with Google.

Has Google or YouTube ever shared the data of Canadians with foreign governments or other jurisdictions?

Ms. Jeanette Patell: Thank you for the question.

I'm actually going to turn to my colleague [*Technical difficulty—Editor*].

Mr. Shane Huntley: Certainly. We publish our transparency reports on government requests about lawful data access, which Jeanette spoke to in her opening statement.

We assess each request under both the U.S. law and the local law and also under international norms. We assess each one and provide data, and then we have transparency reports. We also reveal that if the use of data is provided, we provide that where we are able to under the law.

Mr. Parm Bains: My question was whether the information is shared with foreign governments—other governments.

I'll move on. Maybe this can explain it a bit better. On December 6, U.S. Senator Wyden released a letter: “Unidentified governments are surveilling smart phone users via their apps' push notifications, a US senator warned on Wednesday.... These are the audible 'dings', or visual indicators, which users get when they receive an email or their sports team wins a game.” Most of these “travel over Google and Apple's servers.”

What can you tell us about these government requests for user data?

● (1730)

Mr. Shane Huntley: We are aware of Senator Wyden's letter and [*Inaudible—Editor*]. This was from.... I am not aware of the specifics, and the specifics were not provided with regard to his anonymous source. I would say that anything provided here would fall under the same policies I just spoke about in terms of it needing to be under lawful requests coming from a legal process, which we would assess closely. Any such request would be covered under our transparency reports in terms of—

Mr. Parm Bains: Okay. Thank you.

I'll move on to a similar question for Meta.

Has Meta ever shared the data of Canadians with foreign governments or other jurisdictions?

Ms. Rachel Curran: Thank you for that question.

I'll turn it over to my colleague Mr. Gleicher.

Mr. Nathaniel Gleicher: Thank you for the question.

Not too dissimilar from what our colleagues from Google described, we review lawful requests that we receive from governments around the world. We review them carefully, both under U.S. law and local law and international norms. We push back on requests that are overly broad, and when we do disclose data, we have a report where we share information about any data that was disclosed, but here we're talking about pursuant to lawful requests and responses to those requests.

Mr. Parm Bains: In February, U.S. senators Warner and Rubio wrote a letter to Meta about documents that demonstrate Meta knew that developers in China and Russia had access to user data that could be used for espionage. The letter refers to an internal Meta document, which claims that “90,000 developers in China had been given access to information about users, including profile data, photos and private messages even though Facebook had never been able to operate in China.”

At the time, Meta did not respond to Reuters for a comment. Are you able to do so now?

Mr. Nathaniel Gleicher: I'm not aware of the specifics of this particular instance.

What I can tell you is that we proactively investigate and hunt for cyber-espionage campaigns: efforts by foreign governments to spy on innocent people around the world. We regularly report on that work through our quarterly reports, where we describe the enforcements we've taken, and then we share information about any operations that we do identify with others in industry so they can take action as well.

One of the things we've seen is that these types of campaigns are broad efforts that target the Internet broadly—multiple platforms—and often involve off-platform activity as well. Investigating these, disclosing information on them and then sharing that information with other parties is a really important part of tracking and countering these adversaries.

Mr. Parm Bains: Okay.

With respect to the specifics I outlined there, could you please provide any information that you can in writing to the committee?

Mr. Nathaniel Gleicher: As I said, I'm not aware. I don't know the details of that, but I'd be happy for us to come back with more information.

Mr. Parm Bains: Thank you.

The Chair: Thank you, Mr. Bains.

[*Translation*]

Mr. Villemure, you have the floor for two and a half minutes.

Mr. René Villemure: Thank you, Mr. Chair.

Ms. Curran, I'm going to turn to you again, if I may.

Earlier, you mentioned two major American companies. Would you say that making money is more important than informing people?

[*English*]

Ms. Rachel Curran: Monsieur Villemure, we do think we keep people informed with the credible information we have on our platforms. Additionally, we would be more than happy to bring news content back to our platforms. We believe that we provide a great deal of marketing and distribution value to local news publishers. We'd like to proceed in partnership with them if we can do so under the framework of the current legislation.

[*Translation*]

Mr. René Villemure: Thank you very much.

Would you say that Meta has set an example when it comes to protecting privacy, or is it doing as little as possible to comply with the minimum required by law?

[*English*]

Ms. Rachel Curran: We have totally overhauled our privacy practices in the last number of years, Monsieur Villemure. We really embed privacy considerations at the front end of the design of all of our products and services now. We can go through that in great detail for you if you'd like. Privacy is one of the key considerations now in building anything we offer to the public.

[*Translation*]

Mr. René Villemure: Thank you very much.

On another note, can you define what pornography is for Meta?

[*English*]

Ms. Rachel Curran: Monsieur Villemure, we do not allow sexually explicit material on our platforms. We remove it when we identify it, and we report out on those removal efforts. Through our transparency centre, you can see how many pieces of content we've removed—

● (1735)

[*Translation*]

Mr. René Villemure: Excuse me for interrupting. I understand that you're removing the content in question, but what are your criteria for determining that it's pornography?

[*English*]

Ms. Rachel Curran: We remove content that our systems, our reviewers and our moderators identify as sexually explicit. The definition of that, Monsieur Villemure, is set out in our community standards, which are public. We enforce against content according to the definitions set out in our community standards.

[*Translation*]

Mr. René Villemure: Okay, but it's not very clear.

[*English*]

Ms. Rachel Curran: I'm sorry, Monsieur Villemure. I think I missed that question.

[*Translation*]

Mr. René Villemure: I was saying that it isn't very clear. It's not easy to understand.

[*English*]

The Chair: We are out of time.

Ms. Rachel Curran: We'd be happy to—

The Chair: Ms. Curran, perhaps you could supply the committee with what the standard is.

Ms. Rachel Curran: Yes. I think this is a very important issue, Mr. Brassard. I'd be happy to provide Monsieur Villemure with the definition of sexually explicit material that we use in our community standards and what we remove.

The Chair: Thank you, Ms. Curran. I would suggest that you do that through the clerk so that it can be distributed to the committee.

Mr. Green, you have two and a half minutes.

Go ahead, please.

Mr. Matthew Green: Thank you very much.

Ms. Curran, in your previous testimony, you disagreed, I think, with the characterization in the New York Times article talking about Meta's involvement with youth.

I'll turn your attention to written testimony by Artura Bejar in the congressional Subcommittee on Privacy, Technology, and the Law, dated November 7, 2023. For the record, he was a senior engineer and product leader at Facebook, responsible to keep users safe and supported.

In his written testimony to that congressional hearing, he said that he "sent a detailed email to Mark Zuckerberg" and in it "explained that the number of people reporting to surveys that they had a negative experience on Instagram was 51% every week but only 1% of those reported the offending content and only 2% of those succeeded in getting the offending content taken down." He said he "detailed the staggering levels of abuse that teens aged 13-15 were experiencing every week. The initial data from the research team indicated that as many as 21.8% of 13-15 year olds said they were the target of bullying [within the past week]." There are many more statistics that are put in there.

If you don't agree with the New York Times article, that's fine, but what do you say to your former senior engineer responsible for safety on Facebook, given what I think is an indictment in his written testimony before the congressional privacy hearing?

Ms. Rachel Curran: Thank you, Mr. Green.

Again, we've developed more than 30 new tools and features to support safe and positive experiences for teens and their families, so—

Mr. Matthew Green: When was that developed?

Ms. Rachel Curran: We've developed that over the last couple of years in particular, Mr. Green, but it dates back further than that. These tools I'm referencing now.... For instance, we set teens' accounts to "private" when they join Instagram or Facebook. We prevent adults they don't follow from sending them messages. We limit the amount of potentially sensitive content they can see in "Explore", "Search" or "Reels". We prohibit content that promotes suicide, self-harm or eating disorders—

Mr. Matthew Green: Did these developments happen after October 5, 2021? The whistle-blower in this context stated that it was in 2021. He went on to say that children were receiving "unwanted sexual advances" and that "an even higher percentage of these children are receiving unwanted sexual advances on a monthly basis."

Did these new tools you're talking about happen before or after 2021?

The Chair: Please provide a very quick response, Ms. Curran.

Ms. Rachel Curran: Yes, a lot of these tools were developed recently, in the last couple of years. Youth safety, of course, was a priority long before that, but the tools I am talking about have been developed recently.

The Chair: Thank you, Ms. Curran and Mr. Green.

Again, to our guests, make sure you have your French interpretation on.

[*Translation*]

Mr. Gourde, you have the floor for five minutes.

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

My first question is for the Meta representatives.

During the 2019 and 2021 election campaigns in Canada, there were foreign influence activities carried out on platforms like the ones you manage. The purpose of these activities was to defeat certain candidates. Since these activities fall outside the scope of the Canada Elections Act, which is enforced by Elections Canada, we have no way of knowing whether election spending limits were respected, among other things.

Now that we all know this, for the next federal election, would it be possible for Meta to set up a monitoring period from the time Elections Canada calls the election?

During this 35- or 45-day period, is there a process that allows people who feel they have been wronged to file a complaint?

The Canadian Security Intelligence Service and the Royal Canadian Mounted Police are unable to help us during this period. Should we file a complaint directly on your platforms and send a certified copy to Elections Canada to speed up the process?

● (1740)

[*English*]

Ms. Rachel Curran: Thank you for the question, Mr. Gourde.

In fact, there is no evidence that any foreign interference or influence operations targeting Canadians during the last election were present on our platforms. For more detail on that, I'm going to turn it over to my colleagues, Mr. Gleicher and Dr. Hundley.

Mr. Nathaniel Gleicher: Thank you, Rachel.

Thank you for the question.

We investigate proactively and enforce against any foreign interference operations we identify, and then we publish information about them in our quarterly threat reports. When we publish that information, we also publish details on particular countries or regions that were significantly targeted, and when we do have proof, we will also publish information about who, or what organization, was behind the operation.

We have a dataset that outlines every single influence operation we've identified and removed from our platforms. It is available for download and review, and we would be happy to provide it to the committee. It also includes the information I am describing, to be able to look backwards.

Going forward—

[*Translation*]

Mr. Jacques Gourde: I'm sorry. My next question will be more specific.

For the next election, do you have a process in place that will allow us to file a complaint directly with you if we become aware that there has been foreign influence on one of your platforms, since these activities cannot be monitored by Elections Canada?

How can we work with you to avoid this problem?

[*English*]

Ms. Rachel Curran: Thank you for the question, Mr. Gourde.

Yes, we'd be happy to set up a protocol with policy-makers specifically to do that.

I can tell you that ahead of any election in Canada, we work not only with Elections Canada, but also with Global Affairs and with the Privy Council Office, to make sure we're monitoring and addressing any issues on our platforms, including foreign interference, but we would be happy to set up another or a different protocol with members of Parliament specifically.

[*Translation*]

Mr. Jacques Gourde: You just told us that you collaborated with Elections Canada and the Privy Council in 2019 and 2021, but it doesn't seem to have worked. We've only just learned, barely a year ago, that there have been problems. What you're saying doesn't tally with the reality we've experienced.

Were these protocols already in place in 2019?

[*English*]

Ms. Rachel Curran: They were, Mr. Gourde. In fact, we found no issues and no problems on our platforms during the last couple of elections, including the one in 2019.

We work quite rigorously ahead of those elections, as well as during and afterwards, to monitor for any problems and to remove any problematic content. For instance, we've reported out on that publicly, and we did not see any evidence of foreign interference on Meta platforms during the last election or during the one in 2019.

[*Translation*]

Mr. Jacques Gourde: My question is for the representatives of Google Canada.

For your part, have you observed any foreign influence activities on your platforms during the 2019 and 2021 elections?

[*English*]

Mr. Shane Huntley: I can take that question.

My team tracks very closely foreign interference operations. As I said, we are transparent about what we do detect. We have not detected any interference in Canadian elections on our platform as part of our investigations over the last number of years.

[*Translation*]

Mr. Jacques Gourde: Thank you very much.

My next question is for the representatives of X Corporation.

You acknowledged that the old Twitter was a platform often used to relay fake news.

Is there a protocol to prevent this and speed up the removal of fake news during an election period?

[*English*]

Mr. Wifredo Fernández: There are a couple of interventions that are applicable here. First is our civic integrity policy. Our civic integrity policy targets four areas of potential violations: misleading information that could be misleading about how to participate in an election; misleading information that could intimidate people from participating; information that could suppress the vote; and false affiliations, so impersonation.

Second, we have a product we have been investing a lot of resources in called "Community Notes", which is a decentralized approach for the community on X to add context to content they believe may be misleading in order to help other readers. This allows people on X to become contributors, to rate the helpfulness of these community notes and to write notes.

● (1745)

The Chair: Thank you, Mr. Fernández.

Mr. Wifredo Fernández: You're welcome.

The Chair: Mr. Kelloway, go ahead for five minutes.

Mr. Mike Kelloway (Cape Breton—Canso, Lib.): Thank you, Mr. Chair.

Thanks to the witnesses here today.

My first series of questions will go to Meta and then, if we have time, to Google.

The first one is around the Wall Street Journal. In 2021, they reported that there was a clear link between Instagram and detrimental mental health effects. Can you crystallize the actions taken by Meta since this particular report?

Maybe we could start with Ms. Curran.

Ms. Rachel Curran: Listen, I talked about some of the new tools and features that we have developed to keep teens safe on our platforms and to address any concerns around safety or mental health.

Let me talk about some of the tools we have developed for parents as well. We now have parental tools that let parents and guardians see whom their teen reports or blocks and set blocking hours for when they can use our platforms. We also recently launched the family centre, with expert resources on how to have dialogues with teens about their online habits. We also give teens ways to manage their time on social media so it's intentional and meaningful. We give them the option to set time limits or to turn on "Take a Break" on Instagram, which would remind them to take regular breaks while scrolling through social media. We send teens notifications to remind them of that. We also notify them when it might be time to look at something different if they have been scrolling on the same topic for a while.

Mr. Mike Kelloway: Thank you, Ms. Curran.

I think I will stay with you, if possible. Is there more recent data available on the mental health of users who use Instagram or Facebook? I'm thinking particularly of male and female youth demographics.

Ms. Rachel Curran: Yes. Look, the most recent research that we have doesn't support the hypothesis that digital technology is behind trends in teen mental health and well-being. The existing body of research doesn't rule out other common factors like economic instability, substance use and academic pressure.

There's also a growing body of research that suggests that social media can play a positive role in teens' lives and provide support in particular to those who are struggling or to members of marginalized groups.

We're always reviewing this research and funding external independent researchers to look into these issues, but so far the research is really mixed.

Mr. Mike Kelloway: Thank you very much.

I have one last question for you, Ms. Curran, or for your colleagues at Meta. Are messages on Facebook stored? I want to make sure I get it correctly. Are they stored?

Ms. Rachel Curran: Maybe I'll turn that over to my colleague, Mr. Gleicher. If he doesn't have the answer, we will get back to the committee in writing.

Mr. Nathaniel Gleicher: I think, to give you a full and comprehensive answer, it would be best for us to come back to you in writing on that.

Mr. Mike Kelloway: Okay. That would be wonderful.

Mr. Chair, how much time do I have?

The Chair: You have one minute and 38 seconds.

Mr. Mike Kelloway: Excellent.

We're going to go to Google.

Do voice products, such as Google Assistant and Google Home, have the capability to store recorded audio?

Ms. Jeanette Patell: With devices, they will all have individual settings, so people can make the choices that are right for them.

I think your question was whether the audio could be stored. Is that correct?

Mr. Mike Kelloway: That's correct, yes.

Ms. Jeanette Patell: I think I'll need to get back to you on that.

Mr. Mike Kelloway: That would be great. I mean, if it's a no, that's one thing. However, if it's a yes, I'd like to know why. What is the need for the audio to be stored? If that could be part of the response back, Mr. Chair, that would be appreciated.

● (1750)

The Chair: Thank you, Mr. Kelloway.

[*Translation*]

We have 20 minutes left with the witnesses. If we have the unanimous consent of the committee, I would allow Mr. Villemure and Mr. Green to ask questions. In fact, each party would have five minutes of speaking time. That would bring us to the end of this round of questions.

Is that agreeable? That's fine.

[*English*]

Mr. Barrett, go ahead for five minutes.

Mr. Michael Barrett: We talked, in Ms. Vecchio's questions, about the protection of folks from inadvertent exposure to sexually explicit material. I'm keenly interested, though, in what steps each of your platforms is taking to prevent the transmission or display of sexually exploitative material—sometimes referred to as child pornography—on your platforms.

I think the prevalence of sexually explicit materials, in and of itself.... What each of your respective platforms is doing with respect to age verification is one issue. This is a separate issue from that. Could you each take about 45 seconds to say what active steps you are taking to prevent the facilitation or distribution of sexually exploitative materials of minors on your platform?

We'll do the same order that I went through last time, starting with X Corporation, please.

Mr. Wifredo Fernández: Child sexual exploitation has no place on X, and we're working to make it the most inhospitable place for people who want to distribute child sexual abuse materials. Over the last year, we've been more aggressive in our enforcement of such material on the service, restricting the search for this material, increasing our training for agents to make reports to the cyber tip line, and automating our process for reporting to the cyber tip line for the National Center for Missing & Exploited Children in the United States, which acts as a global clearing house for tip lines in different jurisdictions. We recently announced a product partnership with Thorn to enhance our detection capability.

We're doing a lot in this space. The work continues, but this has zero purpose on our platform.

Mr. Michael Barrett: I have the same question for Meta, please.

Ms. Rachel Curran: Thank you, Mr. Barrett.

We lead the industry in this space. I'm really proud of our work on this front. It's so important. We've developed new technologies to keep this abhorrent abuse off our platforms. In fact, we've removed more than 34 million pieces of child exploitation content from Facebook and Instagram in Q4 of 2022. Over 98% of that was detected before it was reported.

We use a combination of technology and behaviour signals to detect and prevent child grooming or potentially inappropriate interactions between minors and adults. We also help law enforcement find and prosecute the criminals who commit these heinous acts, including by responding to requests for information from law enforcement, providing instructional guidelines and training, and supporting the development of a case management tool for the National Center for Missing & Exploited Children cyber tips.

We've also built long-standing partnerships with anti-trafficking experts and child safety organizations, including organizations like OneChild in Canada, to help protect kids. Other organizations include Thorn, Polaris and Stop the Traffik.

Look, I would say that although we are doing industry-leading work, our work is never done here. It's a highly adversarial space. We know there are a lot of bad actors there, online and off-line. We're going to prioritize our work to protect vulnerable kids.

● (1755)

Mr. Michael Barrett: I appreciate your answer. Thank you.

I have 45 seconds remaining.

This is for Google, with the same question, please.

Ms. Jeanette Patell: Thank you for the opportunity to speak to this because [*Technical difficulty—Editor*] more important than keeping children safe.

At Google and YouTube, in addition to the similar activities of the other platforms in detecting and removing this content, we are also leaders in providing hashes of that content to NCMEC and then freely providing those hashes to other platforms, so that this content cannot be recirculated on other platforms. We work with law enforcement to ensure that perpetrators are prosecuted where possible and as appropriate. We are very focused on not allowing this content on YouTube.

The final thing I'll say on that is that if you look at our policy and community guidelines around nudity and sexually explicit content, you'll notice that in fact they are written in such a way that content that is intended for sexual gratification is prohibited on YouTube. That is informed by our work with external experts in this space.

The Chair: Thank you, Ms. Patell.

Ms. Khalid, you have five minutes.

Go ahead, please.

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

I'll start again with Meta.

This is a yes-or-no question, if that's okay. You did say that Meta is not an essential service. Billions of people use it across the world. Do you think that you have a duty to protect Canadians?

Ms. Rachel Curran: Listen—

Ms. Iqra Khalid: I'm sorry, just say “yes” or “no”, if that's okay. I want to get around to everybody, please.

Ms. Rachel Curran: I'm sorry, but the question is not entirely clear. Protect Canadians from what, Ms. Khalid?

Ms. Iqra Khalid: It's to provide a safe platform for them to be able to use this service that you give to them.

Ms. Rachel Curran: Agreed, and it's to provide credible information on that platform, yes.

Ms. Iqra Khalid: Thank you.

I have the same question for Google. Do you have a duty to protect Canadians on your platform?

Ms. Jeanette Patell: We take our responsibility very seriously. It is our number one priority to provide a responsible and safe platform for all of our users.

Ms. Iqra Khalid: Do you have a duty to protect Canadians on your platform? That's what I'm asking.

Ms. Jeanette Patell: I'm not certain about the precise wording. I would say that we have recognized our responsibility to all partners and users on our platform to have a safe platform for all—

Ms. Iqra Khalid: Who are these partners and users? Are you just talking about the users, the average Canadian who has a Gmail account, a YouTube account, etc.? They're all linked together with all of their data stored in one spot. We don't know exactly where that data is stored.

Are you talking about those people, or are you talking about third party contractors with whom you would potentially be partnering to provide these services to Canadians as well?

Ms. Jeanette Patell: Our responsibility is to all of our partners, whether that is our creators on YouTube, the users of YouTube or advertisers on YouTube. We have built a model where responsibility underpins the entire framework. That is really at its core, how we keep our platform safe for everyone, whether they're in Canada or around the world.

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

I have the same question for X. Do you have a responsibility and a duty to protect Canadians who use your platform?

Mr. Wifredo Fernández: Yes. As the town square, we want people to be able to participate safely in public conversation.

Ms. Iqra Khalid: In a town square, there are often opportunities for mobs to gather. If we're making that analogy, do you, as the owner of the platform, have a responsibility to provide a safe space for Canadians to partake in a public square kind of atmosphere, one that is filled with real information, safe from misinformation and safe from disinformation?

Mr. Wifredo Fernández: Yes, the accuracy of information is of utmost importance. The community notes—

Ms. Iqra Khalid: What about the safety of those who use the platform?

Mr. Wifredo Fernández: Absolutely. Abuse and harassment have no place in a town square.

Ms. Iqra Khalid: I pose to you this: What are you going to do to protect Canadians who are suffering? How are we going to maintain the rights of Canadians, especially those who are of minor age, on the platform that you provide and that so many of us use?

Mr. Wifredo Fernández: We'll continue to rigorously enforce all of our policies that help keep them safe, especially minors.

● (1800)

Ms. Iqra Khalid: Do you think that you also have an obligation to work with governments to create that safe space, all levels of government and community partners?

Mr. Wifredo Fernández: Sure. Compliance with laws all around the world is essential. We want to be thoughtful partners in complying with the laws of different lands, absolutely.

Ms. Iqra Khalid: I think this is going to be my last question.

There was a question that was asked earlier about foreign governments accessing Canadian data. I forget which one of you said that lawful requests of foreign governments seeking access to Canadian data are allowed.

Can you please define what lawful requests of a foreign government accessing Canadian data would be?

The Chair: To whom are you directing that?

Ms. Iqra Khalid: I don't remember who it was.

I would like, perhaps, brief answers from everybody, if that's okay.

The Chair: It was Mr. Gleicher.

Ms. Iqra Khalid: Was it? Then go ahead, Mr. Gleicher, please.

Mr. Nathaniel Gleicher: Whenever we receive a request from law enforcement or governments around the world.... There are a number of international legal frameworks that enable governments to make lawful requests of platforms and of other organizations for information across borders. We review those requests carefully. We push back—

Ms. Iqra Khalid: I'm sorry; I'm going to stop you right there. I'm just looking for a definition of what “lawful request” means. If you can provide that in writing, that would be great.

The Chair: I'm going to suggest that all three of our guests provide that in writing to the clerk. I think it's a really important question that needs to be answered.

Thank you, Ms. Khalid.

[*Translation*]

Mr. Villemure, you have the floor for five minutes.

Mr. René Villemure: Thank you very much, Mr. Chair.

Ms. Curran, don't worry, I'm going to talk to your colleagues.

Mr. Harris, on the subject of foreign interference, could you tell us something we haven't heard here yet?

[*English*]

Mr. Josh Harris: I'm sorry; I want to make sure that I understand the question. Foreign interference in regard to...?

[*Translation*]

Mr. René Villemure: I'm talking about foreign interference in Canadian politics.

[*English*]

Mr. Josh Harris: We have a series of policies that we've discussed at some length today. It involves the protection of all users, including Canadian users, from any outside interference with their data, whether that's illegal hacking activity—

[*Translation*]

Mr. René Villemure: Sorry to interrupt. I know you have a dozen policies. However, what can you tell us about them? What do we not know yet?

[*English*]

Mr. Josh Harris: When you're talking about foreign interference—I want to make sure that I'm as responsive as possible here—are you talking specifically about...? Can you give me a definition of foreign interference?

[*Translation*]

Mr. René Villemure: Thank you, Mr. Harris, but I don't have much time left.

Ms. Hundley, I'm going to ask you the same question. You are responsible for influence operations policy. On the subject of foreign interference, could you tell us something we don't already know?

[*English*]

Dr. Lindsay Hundley: One thing I would highlight is that, as we noted in our latest transparency report earlier this year, we detected and removed a cluster of commenting activities from the influence operation known in the security community as “spamouflage” that targeted audiences in Canada. Researchers at the Australian Strategic Policy Institute have described that this operation's use of likely generative AI audio and doctored YouTube videos shared on other platforms “had zero or minimal engagement with real users.”

Spamouflage is a long-running, cross-Internet operation with global targeting that we and other industry peers have been enforcing on since 2019. In August, we removed thousands of accounts and pages under our CIB policies, after we were able to connect different clusters of activities together to be part of a single operation that we were able to attribute to individuals associated with Chinese law enforcement.

The one thing I will highlight here is that these operations are cross-Internet operations, so this particular activity, known as spamouflage, actually operated on over 50 platforms and forums across the Internet, including Facebook, Instagram, X or formerly Twitter, YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, LiveJournal, Vimeo and dozens of other smaller platforms, so we really believe that countering foreign interference is something that requires a whole-of-society effort.

[*Translation*]

Mr. René Villemure: Thank you very much.

If you could provide that information in writing to the committee, it could be very helpful.

I'm going to put the same question to Mr. Huntley from Google.

● (1805)

[*English*]

Mr. Shane Huntley: Similar to what has already been spoken about, we've also been tracking “Spamouflage Dragon”, also known as “Dragonbridge”.

As has been pointed out, it's important to realize that many of these campaigns may be high in volume but very low in actual effects because of all the efforts to shut them down. It is actually much more difficult to get engagement on platforms as these foreign-coordinated actors than many people realize. I think part of that is due to the strong partnerships that we have, both with governments and across the industry here. This is not the first time many of us have met.

This work will be ongoing. We will apply it across the board and we will continually increase our understanding of this coordinated activity across our platforms.

[*Translation*]

Mr. René Villemure: Ms. Hundley, could the development of artificial intelligence have an effect on foreign interference via social media?

[*English*]

Dr. Lindsay Hundley: That's an important question.

I think it's important to start by just noting what we have seen with regard to AI-generated content from foreign interference operations so far, and here I would note that the use of AI-generated content is not new. Since 2019, we have identified CIB operations on our platforms that have used profile pictures generated by a technique called generative adversarial networks, also known as GAN profiles. This use of AI-generated content doesn't allow these networks to evade our behaviour-based detections. In fact, over two-thirds of the CIB operations that we removed in the last year featured this type of AI-generated content.

We have seen newer operations using the latest generative AI techniques, and there are challenges that we anticipate there, including related to the scale of the content that can be created, but we fundamentally believe, from what we have seen, that a behaviour-based approach is still well suited for identifying covert influence operations early in their life cycle.

The Chair: Thank you, Ms. Hundley.

Dr. Lindsay Hundley: This is because when we see these operations...by the time they post this content, they will have left a lot of behavioural signals that we can still detect, and I'm happy to provide more information on that.

[*Translation*]

Mr. René Villemure: Thank you.

[*English*]

The Chair: I'm sure we would love to hear more about that. Actually, I quite enjoy listening to you speak, Ms. Hundley. You have a lot of knowledge in this area. I can tell.

Mr. Green, you have five minutes. Please, go ahead.

Mr. Matthew Green: Thank you very much, Mr. Chair.

Mr. Chair, through you to Ms. Patell, in referencing Google, a lot of the conversation here today has been centred around the search platform and the public-facing interactions as they relate to the privacy of information.

I'm going to take a step back from that and reference the guiding principles on business and human rights that have been put forward by the Office of the United Nations High Commissioner for Human Rights.

Would you agree that companies have a responsibility to respect standards of international humanitarian law?

Ms. Jeanette Patell: Google is committed to respecting an approach to all of our products and services that puts user safety and privacy at the forefront.

Mr. Matthew Green: Do you have a responsibility to the standards of international humanitarian law?

Ms. Jeanette Patell: I'm not a lawyer, so I'm not in a position to be able to answer that.

Mr. Matthew Green: The international law would state that you do, and it would state that humanitarian law imposes obligations on business managers and staff not to breach the rules of international law.

I bring that up not in the context of your search engine platform but rather in the context of the cloud services that you provide. I want to hear from you on project Nimbus. As you may know, project Nimbus is a cloud computing project by the Israeli government and its military. It has come under condemnation for the use of cloud computing services, including artificial intelligence and machine learning, particularly as the project leads to furthering abuses of Palestinian human rights in the context of the ongoing occupation and the Israeli bombardment of Gaza.

Specifically to that point, I want to ask if you could just elaborate on Google's use of machine learning and artificial intelligence in what have been described by many UN experts as ongoing war crimes and crimes against humanity in Gaza.

Ms. Jeanette Patell: When it comes to project Nimbus, it's not a contract with which I'm personally familiar.

Google has said publicly that it is a project related to workloads that run on our commercial platform by Israeli government ministries such as finance, health care, transportation and education.

When it comes to—

● (1810)

Mr. Matthew Green: Would you agree that the primary contract in the Israeli government is the military and the use of artificial intelligence and machine learning as it relates to surveillance within the occupied Palestinian territories?

Ms. Jeanette Patell: No, I wouldn't agree with that. The work under project Nimbus is not directed at highly sensitive or classified military workloads that are relevant to weapons or intelligence services.

When it comes to our AI systems and products, all of our AI [*Technical difficulty—Editor*] products are anchored in our AI principles, which we were a leader in publishing in 2018, so we've been thinking about responsible AI development for a very long time.

One of the first principles that we have articulated is that AI needs to be developed for socially beneficial purposes designed to avoid reinforcing bias—

Mr. Matthew Green: Is it your testimony here today that your product is not being used for surveillance and unlawful data collection by the Israeli government? Is that your testimony here today?

Ms. Jeanette Patell: As I said, I can't speak to the specifics in that contract or how—

Mr. Matthew Green: Perhaps you could speak to the use of Google Ventures, the venture capital side of Google. Again, it's not a forward public-facing thing, but where the Alphabet company stashes its money. In particular, maybe you could speak to Project Maven and the use of drone technology there. Obviously, many of your former staffers have gone into these types of military contracts, which still have a connection with Google Ventures.

Can you just talk a little bit about Project Maven and its implications?

Ms. Jeanette Patell: Maybe I'll turn to my colleague, Shane Huntley, because again, this is not a project that I'm an expert on.

The Chair: Shane, you have 40 seconds.

Mr. Shane Huntley: My understanding is that Project Maven did not go ahead.

What I would say is that, since that time, we have developed these AI principles, which specifically have undertakings that we are not pursuing—weapons or other technologies for that principal purpose and technologies for specific harm. Since that time, we've been very clear about how we are thinking about AI, and these AI principles underpin everything we do in the space, every product we provide and all of the development we do. These AI principles are the guiding light that we use.

The Chair: Thank you, sir.

I want to thank all our witnesses for being here today as part of this study.

I am going to remind all of you that you will be receiving emails from the clerks with the questions that have been asked by the committee members for you to respond to. I'd like to impose a deadline for those responses of December 20 at 5 p.m. That's one week from today. You should be hearing from the clerk tomorrow at some point.

I'd like to remind members that if they do have questions for any of these witnesses, they should submit them to the clerk by 5 p.m. tomorrow. That way, we can give our witnesses enough opportunity to answer those questions within that week, until December 20.

Thank you, Meta, Google and X, for being here today.

I'm going to dismiss the witnesses, because I do have some committee business that I'd like to discuss. I remind all committee members that we will go in camera. There's an agreement among the parties that this concludes our social media study and that we are going to provide drafting directions to our analysts as well.

Thank you, witnesses, for being here. You are dismissed.

For the purposes of our committee, we haven't yet figured out what the dates of our meetings are going to be, but I did want to list where we are.

I apologize to all committee members. I wasn't able to be here on Monday, but we are working to have the commissioner of the RCMP and the staff sergeant appear as soon as possible when we get back. We're hoping for that to happen the week of the 29th. That is the motion related to SNC-Lavalin.

I remind the committee that the motion for spyware has been approved for up to six meetings. I remind the committee that SDTC is technically done, as far as this committee is concerned, so we are not expected to report to anyone in that motion. I just wanted to remind you of that.

On the draft report for the social media study, we are going to go in camera soon to provide drafting instructions to our analysts. We expect that we could have that report when we get back, so we will have to consider some meetings when we get back to deal with the draft of that report.

That's all I wanted to talk about.

Go ahead, please, Mr. Barrett.

● (1815)

Mr. Michael Barrett: What time are we done, Chair?

The Chair: We're done at 6:40, and we have to go in camera.

Mr. Michael Barrett: With respect to the schedule, you talked about the end of the SDTC study. I've sent a motion to the clerk that I'm going to put forward for the committee's consideration in light of testimony that we heard at another committee this week. I'll be brief in my presentation of it and give committee members an opportunity to consider it and respond.

> That, given the testimony heard from the SDTC whistleblower on Monday December 11, 2023 before the Standing Committee on Industry and Technology, in which the individual states that the Minister of Industry lied before this committee regarding the government's knowledge and handling of serious conflict of interest and misappropriation of taxpayer money, the committee immediately expand its study into SDTC for an additional six meetings, and that the committee hear testimony from the Minister of Industry, the SDTC whistleblower, Officials from the Privy Council Office, Industry Officials, Annette Verschuren, Leah Lawrence, Guy Ouimet, Andrée-Lise Méthot and all other witnesses deemed relevant to the committee's study.

The Chair: Are you giving notice, or are you moving the motion?

Mr. Michael Barrett: I'm moving the motion.

The clerk has it and is able to circulate it in both official languages.

The Chair: Go ahead.

Mr. Michael Barrett: Chair, this week we heard from the whistle-blower in another committee—

Mr. Matthew Green: I have a point of order.

The Chair: Go ahead.

Mr. Matthew Green: I'm wondering if we've been accorded the due time frame for notices. I understood that they need at least 48 hours. Is that correct?

This is not an at-hand motion based on any kind of debate we're currently involved in.

The Chair: Let me double-check with the clerk and get back to you, Mr. Green.

Mr. Matthew Green: Thank you.

The Chair: Mr. Green, we are in committee business, so I am going to rule the motion admissible at this point.

Mr. Matthew Green: Mr. Chair, is it that we don't need to provide notice of motion anymore? Can we table-drop, at any point in time, any motion that we see fit? Is that the ruling of the chair?

The Chair: The fact that we're in committee business.... That is my ruling, Mr. Green. We are in committee business, so I'm going to allow this motion to stand.

Mr. Matthew Green: Mr. Chair, on a point of order, could the clerk reference the standing order that allows us to waive the notice of motion period? I understand that an at-hand motion related to a debate could be put at any time, but I always thought—and I'm happy to be corrected and learn something new here today—that a notice of motion time period is still required in order for the motion to be considered, prior to it being duly put.

The Chair: Thank you for that, Mr. Green.

I am going to refer to the clerk, at this point. Perhaps she can provide some guidance.

There's no specific reference, Mr. Green, to the Standing Orders. It's subject to the chair allowing the motion to be admitted as part of debate. I am determining that, because we are in committee business, I'm giving Mr. Barrett the opportunity to present this motion.

That's the ruling I am making.

● (1820)

Mr. Matthew Green: I'll respect your decision, and I'll be sure to use this as an appropriate tool moving forward.

Thank you.

The Chair: Thank you, Mr. Green.

Go ahead, Mr. Barrett.

Mr. Michael Barrett: Mr. Chair, at a standing committee this week, we had a whistle-blower raise $150 million in misappropriation and serious concerns about the testimony given by a minister of the Crown at this committee. I think it's important that the committee, when planning its agenda, give due regard to this.

Look, we had the former chair of that committee pop smoke and vanish mid-appearance at the industry committee yesterday. We had the chair and CEO both resign from this organization following their appearances at this committee. There have been an awful lot of developments since the motion was first moved, so I think it's important that we put some meetings on the schedule and follow up on the testimony we heard from the whistle-blower on Monday at the industry committee.

Thanks.

The Chair: Thank you, Mr. Barrett.

[*Translation*]

Ms. Fortier, you have the floor.

[*English*]

Hon. Mona Fortier (Ottawa—Vanier, Lib.): Can we go directly to the vote, please?

The Chair: Sure. I don't have anybody else on the list, so—

Mr. Matthew Green: I'm trying to piece this together, Mr. Chair. I apologize. This is a table-drop with 10 minutes left to go in our meeting.

I would like to better understand what's before us here, because I'm just pulling up the stories now. Admittedly, Mr. Chair, I missed whatever revelations happened, so I have a couple of questions.

Is this being covered at the industry committee, the exact same study?

The Chair: My understanding is that it is, Mr. Green.

Mr. Matthew Green: Okay.

Mr. Chair, I would say this. I think it's important to be on the record before any Conservative fundraising campaigns go up talking about a cover-up. This is a conversation that we had at this committee. Many of you will recall that it was the will of this committee to wait until further investigations happened prior to revisiting this.

I'm just going to say this, Mr. Chair. Part of the process that we've been witnessing as a tactic is to have every committee run parallel studies—six, seven, eight, nine, 10 meetings at a time—jamming up our studies. I know that Mr. Villemure has a study that is supposed to happen on our return.

I'm interested in this, Mr. Chair. I want to be on the record so that people can see quite clearly that if this whistle-blower has real merit to the things they're saying around a potential breach of our parliamentary privilege by having a minister, as the allegation says, allegedly lie to this committee, that is a significant thing. That is no small thing. I want to make sure that we give it the seriousness and attention that this type of allegation would require.

What I'm troubled with is that it's 6:30 p.m., 10 or 15 minutes after our meeting was supposed to be done, and we're now involved in a debate on this. I don't want to be rushed into a decision on this very serious allegation that's been made without having had the opportunity to review the materials as presented in the news or without having had the opportunity to hear any type of debate. I am uncomfortable voting on this motion.

Now, I'll just state this for the record: I will abstain from voting on this motion if it moves forward in its current form, as it is. I wanted to put that to the committee, because I'm not present there today. I'm not in the room. I can't have conversations with people, and I prefer to negotiate in an open and transparent way. That's where I stand on this.

Thank you.

The Chair: Thank you for that, Mr. Green.

Ms. Khalid, go ahead.

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

I really take the points that Mr. Green has made with respect to, first, the nature of how this motion is being introduced. It's being table-dropped, basically, at the end of a long day. We're trying to get through committee business and figure out what our schedule will be when we come back from the break.

Knowing and understanding how heavy a schedule we have—Mr. Villemure's study is coming up on January 29—we do need to give priority to things that we've already agreed to. I know that in the past we haven't exactly been doing that. I would like to set that precedent now. We agreed that Mr. Villemure's study will start on January 29. Let's get to it.

In the past, unfortunately, we have cancelled meetings where we could have had some of this work done. Now we're having to push it into the new year. For example, Chair, we have two excellent vice-chairs in Mr. Villemure and Ms. Fortier, to make sure that in the sad instance that you're unwell, the committee work still continues.

I really think that at this point, given that other committees—many, many of them—are studying the exact same issue, it would perhaps be prudent for us, while all of that work is going on, to start with the studies that we've already agreed to as a committee, that we've voted on and that we've said are the priorities of this committee.

I will leave it to my colleagues to see how they want to do this, but I really think that at this time, we should not let our agenda be hijacked. On things that we have already agreed to, let's stay true to our word, Chair.

● (1825)

The Chair: Thank you, Ms. Khalid.

I'm not seeing any other hands up or any debate on the motion by Mr. Barrett.

Do we have agreement on the motion?

No. We don't have agreement.

Madam Clerk, go ahead with the vote.

(Motion negatived: nays 6; yeas 3)

The Chair: I will suspend for a couple of minutes while we go in camera.

[*Proceedings continue in camera*]