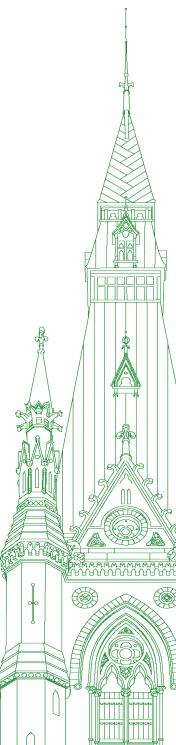44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 135

Thursday, October 24, 2024

Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Thursday, October 24, 2024

● (1545)

[*English*]

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

Good afternoon, everyone.

Welcome, everyone, to meeting 135 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, February 13, 2024, the committee is resuming its study of the impact of disinformation and misinformation on the work of parliamentarians.

I'd like to welcome today's witnesses.

[*English*]

From Google Canada we have Shane Huntley, senior director, threat analysis group, who's joining us by video conference, and Jeanette Patell, who is the director of government affairs and public policy, Canada.

From Meta Platforms Inc., Rachel Curran is here. She is the head of public policy for Canada. We also have Lindsay Hundley, the global threat intelligence lead, who is appearing by video conference.

From TikTok, we have Steve de Eyre, director of public policy and government affairs for Canada, and Justin Erlich, who is the global head of policy development. They are appearing by by video conference.

Also, from X Corporation, we have Wifredo Fernández, who is the head of government affairs, United States of America and Canada.

I welcome you all to the committee for this very important study. As you know, you all have up to five minutes to address the committee.

I will start with Mr. Huntley. Mr. Huntley is online. Can you can go ahead, sir? You have five minutes to address the committee.

Ms. Jeanette Patell (Director, Government Affairs and Public Policy, Canada, Google Canada): Hi there. I'll be addressing the committee on behalf of Google Canada.

The Chair: I apologize.

Go ahead. Thank you.

[*Translation*]

Ms. Jeanette Patell: Thank you very much, Mr. Chair.

Members of the committee, my name is Jeannette Patell. I'm responsible for government affairs and public policy at Google in Canada.

[*English*]

I'm pleased to be joined remotely today by my colleague Shane Huntley, a senior director of Google's threat intelligence group.

Earlier this year, as part of our ongoing commitment to protect elections, Google created the Google threat intelligence group which brings together the industry-leading work of our threat analysis group and the Mandiant intelligence division of Google Cloud.

Google threat intelligence helps identify, monitor and tackle threats ranging from coordinated influence operations to cyber-espionage campaigns across the Internet. On any given day, TAG, the threat analysis group, tracks and works to disrupt more than 270 government-backed attacker groups from more than 50 countries. It publishes its findings each quarter. Mandiant similarly shares its findings on a regular basis, and has published more than 50 blogs to date this year alone, analyzing threats from Russia, China, Iran, North Korea and the criminal underground. We have shared some of our recent reports with this committee, and Shane will be happy to answer your questions about these ongoing efforts.

Google's mission is to organize the world's information and make it universally accessible and useful. We recognize this is especially important when it comes to our democratic institutions and processes. We take seriously the importance of protecting free expression and access to a range of viewpoints. We recognize the importance of enabling the people who use our services to speak freely about the political issues most important to them.

When it comes to the integrity and security of elections, our work is focused on three key areas. First and foremost is continuing to help people find helpful information from trusted sources through our products, which are strengthened through a variety of proactive initiatives, partnerships and responsible safeguards. Beyond designing our systems to return high-quality information, we also build information literacy features into Google Search that help people evaluate and verify information, whether it's something they saw on social media or heard in conversations with family or friends.

For example, our About This Image feature in Google Search helps people assess the credibility and context of images they see online by identifying an image's history and how it has been used and described on other web pages, as well as identifying similar images. We also continue to invest in state-of-the-art capabilities to identify AI-generated content. We have launched SynthID, an industry-leading tool that watermarks and identifies AI-generated content in text, audio, video and images. On YouTube, when creators upload content, we now require them to indicate whether it contains altered or synthetic materials that appear realistic, which we then label appropriately.

We will soon begin to use C2PA's Content Credentials, a new form of tamper-evident metadata, to identify the provenance of content across Google Ads, Google Search and YouTube and to help our users identify AI-generated material.

When it comes to our own generative AI tools, out of an abundance of caution we're applying restrictions on certain election-related queries on Gemini and connecting users directly to Google Search for links to the latest and most accurate information.

The second area of focus is working to equip high-risk entities, like campaigns and elected officials, with extra layers of protection. Our advanced protection program and Project Shield are free services that leverage our strongest set of cyber protections for high risk individuals and entities, including elected officials, candidates, campaign workers and journalists.

Finally, we focus on safeguarding our own platforms from abuse by actively monitoring and staying ahead of abuse trends through the enforcement of our long-standing policies regarding content that could undermine democratic processes.

Maintaining and enforcing responsible policies at scale is a critical part of how we protect the integrity of democratic processes around the world. That's why we've long invested in cutting-edge capabilities, strengthened our policies and introduced new tools to address threats to election integrity. At the same time, we continue to take steps to prevent the misuse of our tools and platforms, particularly attempts by foreign state actors to undermine democratic elections.

The Google Threat intelligence teams, including the threat analysis group founded by my colleague Shane Huntley, are central to this work. They often receive and share important information about malicious activity with national security agencies and local law enforcement, as well as our industry peers, so that they can investigate and take appropriate action.

Maintaining the integrity of our democratic processes and institutions is a shared challenge. Google, our users, industry, law enforcement and civil society all have important roles to play, and we are deeply committed to doing our part to keep the digital ecosystem safe and reliable.

● (1550)

We look forward to answering your questions and continuing our engagement with this committee as you study these important questions.

The Chair: Thank you, Ms. Patell.

Ms. Curran, we're going to go to you for five minutes, please.

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

Lindsay will speak on behalf of Meta Platforms.

Dr. Lindsay Hundley (Influence Operations Policy Lead, Meta Platforms Inc.): Thank you for the opportunity to have us appear before you today.

My name is Dr. Lindsay Hundley, and I am the global threat intelligence lead at Meta. My work is focused on producing intelligence to identify, disrupt and deter adversarial threats on our platforms. I've worked to counter these threats at Meta for the past three years, and my work at the company draws on over 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 University and Harvard Kennedy School.

I'm joined today by Rachel Curran, the head of public policy for Canada.

At Meta, we work hard to identify and counter foreign adversarial threats, including hacking and cyber-espionage campaigns as well as influence operations—what we call coordinated inauthentic behaviour, or CIB. Meta defines CIB as any coordinated effort to manipulate public debate for a strategic goal in which fake accounts are central to the operation. CIB occurs when users coordinate with one another and use fake accounts to mislead others about who they are and what they are doing.

At Meta, we believe that authenticity is a cornerstone of our community. 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 create a space where people can trust the people and communities that they interact with on our platforms.

We also know that threat actors are working to interfere with and manipulate public debate. They try to exploit societal divisions, promote fraud, influence elections and target authentic social engagement. Stopping these bad actors is one of our highest priorities, and that is why we've invested significantly in people and technology to combat inauthentic behaviour at scale.

The security teams at Meta have developed policies, automated detection tools and enforcement frameworks to tackle deceptive campaigns, 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 after creation. Just this year, Meta has disabled nearly two billion fake accounts, and the vast majority, over 99%, were identified proactively.

Our strategy to counter these adversarial threats has three main components. First there are expert-led investigations to uncover the most sophisticated operations. Second is public disclosure and information-sharing to enable cross-societal defences, and third are product and engineering efforts to build the insights derived from our investigations and turn them into more effective, scaled and automated detection and enforcement.

A key component of this strategy is our public quarterly threat reports. Since we began this work, we've taken down and disclosed more than 200 covert influence operations from 68 countries that operated in 40 languages, from Amharic to Urdu to Russian to Chinese. 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.

We've also shared detailed technical indicators linked to these networks in a public-facing repository hosted on GitHub, which contains more than 7,000 indicators of influence operations activity across the Internet.

Before I close, I'd like to touch on a few trends that we're monitoring in the global threat landscape.

To start, Russia, Iran and China remain the top three sources of foreign interference networks globally. We have removed nearly 40 operations from Russia that target audiences around the world, including four new operations in just this past quarter. Russian-origin operations have become overwhelmingly one-sided over the past two years, pushing narratives to support those who are less supportive of Ukraine.

Likewise, China-origin operations have evolved significantly in recent years to target broader, more global audiences, including in languages other than Chinese. These operations have continued to diversify their tactics, including targeting critics of the Chinese government, attempting to co-opt authentic individuals and using

AI-generated news readers in an attempt to make fictitious news outlets look more legitimate.

Finally, we've seen threat actors increasingly decentralize their operations to withstand disruptions from any singular platform. We've seen them outsource their deceptive campaigns increasingly to private firms. We are also seeing them leverage generative AI technologies to produce higher volumes of original content at scale, though their abuse of these technologies has not impeded our ability to detect and remove these operations.

● (1555)

I would be happy to discuss any of these trends in more detail.

I want to close by saying that countering foreign influence operations is a whole-of-society effort, which is why we engage with our industry peers, independent researchers, journalists, government and law enforcement.

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

The Chair: Thank you, Ms. Hundley.

Mr. de Eyre, you have up to five minutes to address the committee. Go ahead, sir.

Mr. Steve de Eyre (Director, Public Policy and Government Affairs, TikTok Canada): Good afternoon, Mr. Chair and committee members. My name is Steve de Eyre. I'm the director of public policy and government affairs for TikTok Canada. I'm joined today by my colleague Justin Erlich, the global head of policy development for TikTok's trust and safety team. He's joining virtually from California.

Thank you for the invitation to return to your committee today to speak about the important issue of protecting Canadians from disinformation. The topic of today's hearing is important to us, to the foundation of our community and to our platform.

TikTok is a global platform where an incredibly diverse range of Canadian creators and artists have found unprecedented success with global audiences; where indigenous creators are telling their own stories in their own voices; and where small businesses like Hamilton's DSRT Company, Mississauga's Realm Candles, and of course Smiths Falls' McMullan Appliance and Mattress are finding new customers, not just across Canada but also around the world.

Canadians love TikTok because of the authenticity and positivity of the content, so it's important, and in our interest, to maintain the security and integrity of our platform. To do this, we invest billions of dollars into our work on trust and safety. This includes advanced automated moderation and security technologies and thousands of safety and security experts around the world, including content moderators here in Canada. We also employ local policy experts who help ensure that the application of our policies considers the nuances of local laws and culture.

When it comes to misinformation and disinformation, TikTok takes an objective and robust approach. To start, our community guidelines prohibit misinformation that may cause significant harm to individuals or society, regardless of intent. To help counter misinformation and disinformation, we work with 19 independent fact-checking organizations to enforce our policies against this content. In addition, we invest in elevating reliable sources of information during elections, during unfolding events and on topics of health and well-being.

We relentlessly pursue and remove accounts that break our deceptive behaviour rules, including covert influence operations. We run highly technical investigations to identify and disrupt these operations on an ongoing basis. We have removed thousands of accounts belonging to dozens of networks operating from locations around the world. We regularly report on these removals in our publicly available transparency centre.

Addressing disinformation is an industry-wide challenge that requires a collaborative approach and collective action, including both platforms and government. At the heart of this collaboration lies transparency and accountability, which we believe are essential to fostering trust. We're committed to leading the way when it comes to being transparent in how we operate, moderate and recommend content, empower users, and secure our platform. As part of this commitment, TikTok regularly publishes transparency reports to provide visibility into how we uphold our community guidelines; how we respond to law enforcement requests for information, or government requests for content removals; and attempts at covert influence operations that we have disrupted on our platform.

Our commitment to transparency is also guiding our work with Canadian officials, including in the national security review of TikTok under the Investment Canada Act. We have been working with officials to ensure that they understand how our platform operates, including how we protect Canadians' user data and defend against things like disinformation and foreign interference. As part of this process, last year we offered Canadian officials the opportunity to review and analyze TikTok's source code and algorithm. While the government has not yet taken us up on this opportunity, we are hopeful that they will do so. We will continue to work collaboratively with the government in the best interest of Canadians.

Such collaboration will be critical as we approach the next federal election. In 2021 TikTok worked with Elections Canada to build an in-app hub that provided authenticated information on when, where and how to vote. That year we were also the only new platform to sign on to PCO's Canada declaration on electoral integrity online. As we approach the next election, we will be building upon these efforts and leveraging learnings and best practices from other elections taking place around the world, including in the U.S.

Finally, I'd be remiss not to mention that today's meeting is taking place during Media Literacy Week, an annual event promoting digital media literacy across Canada. As well, yesterday was Digital Citizen Day, a day that encourages Canadians to engage and share responsibly online. Education plays a critical role in empowering Canadians to be safe online and build resilience against misinformation and disinformation.

In Canada these events are led by MediaSmarts, a Canadian non-profit and a global leader in this space whose work TikTok is very proud to support.

● (1600)

We look forward to sharing more with you about how we are addressing these important issues.

Thank you again for the invitation to speak with the committee today.

The Chair: Thank you, Mr. de Eyre.

We're going to X now. Mr. Fernández, you have five minutes to address the committee.

Go ahead, please.

● (1605)

The Chair: Thank you, Mr. Fernández.

Thank you to all our witnesses for their opening statements.

Members of the committee, we are fortunate that we have all four of the major players on social media here today, which poses its own problems. I'm going to ask every member to direct their questions specifically to an individual. That will save us some time in guessing who's going to answer.

It's been common practice at this committee that we reset after the first set of questions to allow Mr. Villemure and Mr. Green the opportunity to establish those six-minute questions in the second round. Is it the will of the committee to do that?

Some hon. members: Agreed.

The Chair: Thank you.

We're going to start with six minutes of questions.

Mr. Cooper, you have the floor. Go ahead, sir.

Mr. Wifredo Fernández (Head of Government Affairs, United States of America and Canada, X Corporation): Chairman Brassard, Vice-Chairs Fisher and Villemure and members of the committee, thank you for the opportunity to be with you here today. It's an honour.

My name is Wifredo Fernández, and I have the pleasure of leading government affairs and public policy at X in the U.S. and Canada.

We know that X is a critical platform in the public debate around elections. Through September this year, there were over 850 billion impressions, 79 billion video views and four billion posts related to politics globally. We are proud that our platform powers democratic discourse around the world. For us, authenticity, accuracy and safety are fundamental to our approach to elections.

Our consideration of authenticity has two principal dimensions: accounts and conversations. Our safety team proactively monitors activity on our platform and employs advanced detection methodologies to enforce our rules related to authenticity, such as platform manipulation, spam, and misleading and deceptive identities. Whether they are state-affiliated entities engaged in covert influence operations or generic spam networks, we actively work to thwart and disrupt campaigns that threaten to degrade the integrity of the platform.

Through our verification program, we have profile labels that signal the authenticity of accounts, including brands and governments. The grey check mark helps the public know when they are hearing from or interacting with a verified government actor, whether they're an elections official, law enforcement or their representatives.

We want X to be the most accurate source of information on the Internet. That's why we have deeply invested in the development and expansion of Community Notes, which now empower over 800,000 contributors in 197 countries and territories to add helpful context to posts, including advertisements.

A recent study from the University of Giessen in Germany found that across the political spectrum, Community Notes were perceived as significantly more trustworthy than traditional, simple misinformation flags. It also found that Community Notes had a greater effect on improving people's identification of misleading posts. Separate studies from the University of Giessen and the University of Luxembourg show that posts with notes are shared 50% to 61% less and deleted 80% more. We'd be happy to submit these studies for the record.

Deepfakes, shallowfakes, AI-generated photos, out-of-context media and similar content are a source of public concern. This past year, we put a new superpower into contributors' hands, allowing them to write notes that are automatically shown on posts with matching media. To give you a sense of the multiplying effect this has, the around 6,800 media notes that have been written are now showing on over 540,000 posts and have been seen nearly two billion times.

We've also introduced, due to popular demand, the ability for anyone to request a Community Note. With enough requests, top contributors will be alerted and can propose notes. For everyone on X, it's a way to help. For contributors, it's a way to see where help is needed. Posts with a Community Note are also demonetized.

We strongly believe that freedom of speech and safety can and must coexist. The election context brings a diverse set of challenges covering abuse and harassment, violent content, deceptive identities and impersonation, violent entities, hateful conduct, synthetic and manipulated media, and misleading information about how to participate and vote.

At X, every year is an election year, and our policies and procedures are constantly being revised to address evolving threats, adversarial practices and malicious actors. For us, planning begins well in advance of these elections. All relevant working groups internally collaborate to lend their expertise and experience in planning and to participate in enforcing these rules before, during and after elections. We continue to invest in our team and our technology to strengthen our capabilities.

Our efforts extend well beyond content moderation and include proactive initiatives to direct those on our platform to authoritative and reliable sources around election participation. We engage directly with regulators, political parties, campaigns, candidates, civil society, law enforcement, security agencies and others to ensure that clear lines of communication are established to broaden our visibility into the threat landscape and ensure that external partners have a resource here at X.

For example, on multiple occasions over the last year, we engaged productively with Canada's rapid response mechanism and as a result took down networks of accounts, including those linked to the Chinese information operation called "spamouflage". We appreciate the helpfulness of the mechanism and will continue to maintain open lines of communication in the lead-up to the next federal election in Canada.

Thank you again for the opportunity to be with you today. I look forward to any questions you may have.

Mr. Michael Cooper (St. Albert—Edmonton, CPC): Thank you, Mr. Chair. Thank you to the witnesses.

I'll start with Mr. Fernández.

Which foreign state is the most active in spreading or attempting to spread disinformation in Canada on your platform?

● (1610)

Mr. Wifredo Fernández: From our experience over the past year, the "spamouflage" campaign, which is linked to China, has been the most active.

Mr. Michael Cooper: Speaking of the spamouflage campaign, it was detected by, or at least was reported on, by the rapid response mechanism at Global Affairs. It involved a campaign that began in late August and intensified into, I believe, October of last year. It targeted dozens of MPs by falsely accusing these MPs of various ethical and criminal violations.

Is that correct? Is that what you're referring to?

Mr. Wifredo Fernández: Yes. Over the last year, we've taken down about 60,000 accounts linked to the spamouflage operations. About 9,500 of those came from escalations from the rapid response mechanism.

Mr. Michael Cooper: The rapid response mechanism brought those 9,000 to X's attention.

Mr. Wifredo Fernández: That's correct.

Mr. Michael Cooper: Okay.

I will turn to Meta now to maybe address the spamouflage campaign, because Facebook was also used.

Perhaps you could elaborate on the steps you've taken and Meta's interactions with the rapid response mechanism.

Ms. Rachel Curran: I can, absolutely. I'll turn to my colleague, Dr. Hundley, to speak more about this.

Dr. Lindsay Hundley: We've been enforcing against spamouflage since 2019. Last year, we did a really large enforcement under our coordinated inauthentic behaviour policy.

Spamouflage is a long-running, cross-Internet operation with global targeting. We removed thousands of accounts and pages after we were able to connect different clusters of activity together as part of a single operation and were able to attribute that operation to individuals associated with Chinese law enforcement.

We've identified over 50 platforms and forums that spamouflage has used, including Facebook, Instagram, X, YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, LiveJournal, VKontakte, Vimeo and dozens of other smaller platforms and forums.

As with other China-origin operations, we have not found evidence of spamouflage getting significant substantial engagement among authentic communities on our services. As it is a global operation, we have seen targeting of audiences in Canada as part of this targeting. Researchers at the Australian Strategic Policy Institute, for instance, have described the operation's use of generative AI audio and doctored YouTube videos that were shared on other platforms with zero or minimal engagement from real users.

We've engaged a couple of times with the rapid response mechanism, including just yesterday, about spamouflage activity. I'm happy to report that in that instance, they found that we had been able to proactively remove the vast majority of activity that they were tracking.

Mr. Michael Cooper: Going back to the specific spamouflage campaign that I referenced, which occurred last year and was specifically targeting MPs, what was the scale of that campaign on the Facebook platform, and what was the response from the rapid response mechanism vis-à-vis Facebook?

Dr. Lindsay Hundley: Unfortunately, I cannot give you specific numbers on the scale of that one specific campaign, because spamouflage consists of thousands of accounts. They drop in and out of different campaigns overall.

That said, when we engaged with the rapid response mechanism, we had already been tracking a lot of the activity they had shared with us and had removed a lot of it, although information sharing from government partners like these is of course really helpful for identifying anything that does get past our automated detection systems.

Mr. Michael Cooper: On a different note, but to Meta, it was revealed at the public inquiry that during the 2019 election, the Prime Minister's department, the PCO, asked Facebook to remove a Buffalo Chronicle article on Justin Trudeau on the basis that it contained disinformation and that it risked threatening the integrity of the election. In response, Facebook removed the post.

Was Facebook contacted by the Prime Minister's department in the 2021 election with any request to take down Beijing-directed disinformation targeting now former Conservative member of Parliament Kenny Chiu?

● (1615)

Dr. Lindsay Hundley: I am not aware of any of those requests, but this is something that we can check with our internal teams and can get back to you on.

Mr. Michael Cooper: It's now been established that during the 2021 election, the Beijing regime launched a sophisticated disinformation campaign using various social media platforms with the goal of defeating certain Conservative candidates and re-electing Justin Trudeau.

Was Facebook contacted by the Prime Minister's department to take down disinformation about then Conservative leader Erin O'Toole?

Ms. Rachel Curran: I can chime in here, Dr. Hundley, and you should comment as well.

To my knowledge, we were not contacted by anyone in the Privy Council Office or at Global Affairs.

Mr. Michael Cooper: That related as well more broadly to the disinformation campaign directed by Beijing that was targeting Conservatives.

The Chair: Provide a quick response, please.

Ms. Rachel Curran: Yes, that's correct.

The Chair: Thank you, Mr. Cooper.

Just for the sake of the witnesses as well, we're limited on time for questions and answers, so don't take any offence if any of the members reclaim their time from you in the middle of a response. I just want to make that clear.

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

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

My questions are directed to Mr. Fernández, who is representing X today.

I appreciate your providing statistics in your opening remarks today. Here is another one. A 2021 study found that in five G7 countries, Twitter had a "statistically significant difference favoring the political right wing." The study found that Canada had the largest discrepancy between the right and left, with Liberals having an amplification of 43% compared to 167% for Conservatives.

Why does X favour right-wing politicians?

Mr. Wifredo Fernández: Our mission, our operations and our ethos are politically agnostic. Our algorithms actually don't factor in political sentiment in how they recommend content.

Ms. Iqra Khalid: I will ask you this: Does X provide financial support to any Conservative or right-wing politician in Canada?

Mr. Wifredo Fernández: X does not engage in any political giving anywhere in the world.

Ms. Iqra Khalid: In May of this year, X announced that it would be funding Pierre Poilievre's Conservative candidate Matt Strauss in his lawsuit with a Canadian university over vaccine misinformation.

Matt Strauss has been active on X, promoting anti-establishment conspiracy theories and claiming that the World Economic Forum, the WEF, is directing government policy, and he is spreading vaccine misinformation on Russian propaganda channel RT.

How much financial support has been received to date by this Pierre Poilievre Conservative candidate from X?

Mr. Wifredo Fernández: Again, X does not engage in any political giving.

Ms. Iqra Khalid: I am not sure why you are saying that, because X has gone on the record to say that it is footing the legal bills for this person.

I would ask you then, again, are there any other politicians in Canada, whether at the federal, provincial or municipal levels, whom X has supported financially?

Mr. Wifredo Fernández: No.

Ms. Iqra Khalid: How much financial support has been provided to Canadian politicians, in general, by X here in Canada?

Mr. Wifredo Fernández: Again, X does not engage in political giving.

Ms. Iqra Khalid: Does X have mechanisms in place to ensure that any money that has been provided, whether it's to your knowledge or not—and I am hoping that you will come back with that information—is being used for the intended purposes?

As I said, Mr. Fernández, it is on the record that X has agreed that it is footing the bill for this Conservative candidate for the legal fees. I would like to know more information about X's involvement with our Canadian democratic process.

Mr. Wifredo Fernández: I'm happy to follow up with more information on our efforts around the world to support folks who are dealing with issues of freedom of speech, but we do not engage in political giving or in political campaign giving.

Ms. Iqra Khalid: Chair, there is a discrepancy between the information that is publicly available and has been published by X—since it has claimed and confirmed it is footing the bill for a right-wing candidate of the Pierre Poilievre Conservative Party—and what Mr. Fernández has said today.

Given that there is a clear contradiction in what he's saying, I would like, hopefully with the consent of all of our committee, for documents with the following information to be produced: the names of all Canadian politicians who have received financial support from X; how much financial support has been received to date by each of those candidates or elected officials; how much financial support each is entitled to receive; the mechanisms in place to ensure that all money is going to the intended purposes for which there have been commitments made by X to these candidates; proof that all money to date has gone to these intended purposes and that checks and balances are functioning; and, lastly, the status of all legal proceedings for all of the above that I've referred to.

● (1620)

The Chair: You seem to be privy to information that neither I nor any of the other members have, so I don't see any problem with that type of information being requested.

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): I have a question.

The Chair: Okay.

I'm going to stop the clock for Ms. Khalid here.

What's your question, Mr. Barrett?

Mr. Michael Barrett: We would have to know that those documents exist for the committee to be able to request them. The committee does not have the power to request documents that don't exist or to request the creation of documents.

If this is a motion that Ms. Khalid is putting forward—

Ms. Iqra Khalid: I can respond to that, Chair.

Mr. Michael Barrett: —we'd like to see the motion in writing, because without knowing that these documents exist, to your point, Chair, I'm not really sure what the source of this is.

The Chair: Okay.

Mr. Michael Barrett: Let's see what the request is, and then we can consider it, but we're not able to provide unanimous consent for the committee to do something that the committee doesn't have the power to do.

Ms. Iqra Khalid: I'll quote you on that later.

The Chair: That's an interesting point.

Can we deal with this later?

Ms. Iqra Khalid: Absolutely.

Chair, I do want to make a point here, because I feel that—

The Chair: I'm starting your clock again, then, because you're making a point.

Go ahead.

Ms. Iqra Khalid: Absolutely.

To respond to Mr. Barrett's concerns, I will read a tweet from X on May 3, 2024, that says:

> X is proud to fund a lawsuit filed by Dr. Matthew Strauss, an Ontario critical care physician and professor, against his former employer, Queen's University.
>
> After Dr. Strauss argued against wide COVID lockdowns and mandates on his X account...Queen's University...publicly ostracized him, retaliated against him, and ultimately forced him to resign because his opinions did not conform to the university's political orthodoxy.
>
> X supports Dr. Strauss's efforts to vindicate his free speech rights without fear of unfair retaliation!

Knowing and understanding that this person was a candidate for a political party, I want to know why it is that a platform claiming they are protectors of free speech—given the study that I cited earlier—is interfering in the Canadian political democratic process.

The Chair: Okay, your time's up.

I will give Mr. Fernández an opportunity to quickly respond to that, and then we'll circle back to the information you're asking for later.

Mr. Wifredo Fernández: Our company and its leadership have made clear that if there are people around the world whose employment has been affected by what they've said on the platform in exercising their free speech, we will support them by helping defend them. That is what that is linked to. I just want to make that point.

The Chair: Thank you, Ms. Khalid.

[*Translation*]

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

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

Thank you all for being here today.

I'm going to start by asking Ms. Curran my first question.

We've already had the opportunity to exchange views on this subject. A number of experts have told us that disinformation in Finland has been defeated, if you like. At least, it has been greatly affected by the fact that education has been provided. Secondly, the country has a very strong media. They are independent and free. As you know, in Canada, local media have been very affected by Facebook's decision not to sign up to the recent law. I see all the efforts Meta is making to counter disinformation, but, according to our specialists, one of the biggest recommendations is the presence of strong, free media, which you don't subscribe to.

I'd like to know where you stand on this issue.

● (1625)

[*English*]

Ms. Rachel Curran: Look, we've long been clear that the only way we could reasonably comply with the Online News Act is by ending news availability in Canada. That's not a decision we wanted to take. We would be happy to put news back up on our platforms if we were scoped out of the Online News Act or if that bill were repealed.

I should also point out that people in Canada can continue to access news online by going directly to news publishers' websites, downloading mobile news apps and subscribing to their preferred

publishers. There's also a lot of credible information on our platforms, government websites, non-profit websites, politicians' pages and communications and charitable organizations' pages. All of that information is still available.

[*Translation*]

Mr. René Villemure: As you know, the traditional media are used to being on Facebook. So it's their own fault, in my opinion.

The fact remains that one of the first suggestions is to allow strong, independent media to exist. You ask to be exempt from the new law. This is a very important point. I understand your point of view. That said, we are studying disinformation and we realize that your position indirectly encourages it. I'm not accusing you of facilitating disinformation, but people continue to get their information from Facebook instead of from official media sites.

[*English*]

Ms. Rachel Curran: Look, you know, we are actually complying with the Online News Act.

Our removal of news from our platforms was our compliance with that piece of legislation, and we are and were proud of the role we played to support a healthy and diverse news ecosystem.

We had a lot of private deals in place with publishers across Canada, which we had to terminate when the Online News Act came into force, and our free tools and services created pathways for local publishers to connect with their communities. We estimate that this generated more than $230 million in value for Canadian publishers every single year.

[*Translation*]

Mr. René Villemure: Thank you.

[*English*]

Ms. Rachel Curran: Listen, MP Villemure, we would love to restore that value to Canadian publishers, including publishers in Quebec.

[*Translation*]

Mr. René Villemure: Thank you very much, Ms. Curran.

Mr. Fernández, the social media business model is based on the number of clicks; that's no secret to anyone. The algorithm makes its own choices. Personally, I go to the platform X regularly, and it seems to me to be a hostile environment. I've noticed that brutality, banalities and other forms of falsehood generate more clicks than anything of public interest. You can't not know that.

In your opinion, how might we resolve the paradox between the need for clicks for revenue purposes and the hostile environment this currently creates? I have to say, every time I finish my visits to your platform, I get depressed.

[*English*]

Mr. Wifredo Fernández: X has a few different lines of business. We have an advertising business, but we also have a growing business around subscriptions. X Premium and X Premium+ give individual users a suite of tools and advanced analytics and so on that they're able to utilize.

That's a growing part of our business so that we become less reliant on traditional advertising. In fact, X Premium+ has no advertising, which is an advanced feature.

[*Translation*]

Mr. René Villemure: Mr. Fernández, some researchers testified before the committee. They said that X was the worst social media for disinformation.

What do you say to these researchers who unanimously asserted such a thing?

[*English*]

Mr. Wifredo Fernández: I've spoken about our development of Community Notes, which is a novel intervention when it comes to misleading information, and this really puts an incredible power in the hands of our users to add context to posts when they feel it would be helpful to have more context.

This is, I think, a first-in-industry type of product that really, as the research shows, helps combat disinformation, because people are less likely to share that content. That account is demonetized. They are not incentivized to share misleading information because they may receive Community Notes. Then those posts may be demonetized and people are more likely to delete those posts, so it's been an effective tool in that regard.

● (1630)

[*Translation*]

The Chair: Thank you, Mr. Villemure.

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Mr. Green, you have six minutes.

Just to try to be fair to everyone on time, I have to keep tight timelines here. We've gone over on a couple of rounds of questioning, so I'm going to keep it tight.

Go ahead, Mr. Green, for six minutes.

Mr. Matthew Green (Hamilton Centre, NDP): Ms. Curran, your biography on the Canada Strong & Free Network states that you're a lawyer by trade and training and have 15 years of experience in public affairs, including policy advice to the Prime Minister of Canada. You were the director of policy under Prime Minister Harper. Is that correct?

Ms. Rachel Curran: Yes, and I'm very proud of that work, MP Green.

Mr. Matthew Green: Ms. Curran, in the last five years, your biography lists that you worked as a senior associate with Harper & Associates. Is that correct?

Ms. Rachel Curran: That's correct, MP Green.

Mr. Matthew Green: Are you still involved with Harper & Associates in any way?

Ms. Rachel Curran: I am not, no. I have been with Meta now for almost five years—

Mr. Matthew Green: I'm going to reclaim my time. Thank you. In this role, it states that you worked with foreign affairs. Is that correct?

Ms. Rachel Curran: Do you mean in my role with Harper & Associates?

Mr. Matthew Green: No, I mean for Harper when he was in government. You were a senior adviser, including for issues on foreign affairs. Is that correct?

Ms. Rachel Curran: That's correct. I was Mr. Harper's director of policy for a number of years.

Mr. Matthew Green: Ms. Curran, I'm holding a report from Human Rights Watch that is entitled "Meta's Broken Promises—Systemic Censorship on Palestine Content on Instagram and Facebook." The opening line states that "Meta's policies and practices have been silencing voices in support of Palestine and Palestinian human rights on Instagram and Facebook in a wave of heightened censorship of social media amid the hostilities between Israeli forces and Palestinian armed groups that began on October 7, 2023."

Are you familiar with this report?

Ms. Rachel Curran: I'm not familiar with that report.

Mr. Matthew Green: I'll continue to read from it. It says that it reviewed over a thousand cases that involved what they consider to be peaceful content in support of Palestine that was censored or otherwise unduly suppressed, while one case involved the removal of content that was in support of Israel, so essentially there were 1,049 cases of Palestinian suppression and one case in support of Israel.

Human Rights Watch found that censorship of content related to Palestine on Instagram and Facebook was systemic and global and that Meta's inconsistent enforcement of its own policies led to erroneous removal of content about Palestine.

In fact, I believe Meta publicly apologized. They had received some recommendations on patterns of undue censorship; removal of posts, stories and comments; suspension or permanent disabling of accounts; restriction on the ability to engage with content—so shadow banning—and restrictions on the ability to follow or tag.

In response to that, it appears that Meta took responsibility, publicly apologized, and then engaged in business social responsibility by commissioning an independent entity to investigate this. They came back with findings that there appeared to be adverse human rights impacts on the rights of Palestinian users.

Then what has Meta done since to ensure that Meta's practices don't unduly harm the basic freedom of expression for people posting about the question of Palestine?

Ms. Rachel Curran: Thank you for that question. It's a really important one.

Look, since the terrorist attacks by Hamas last October and Israel's response in Gaza, expert teams from across our company have been working around the clock to monitor our platforms while protecting people's abilities to use our apps to shed light on important developments happening on the ground.

We quickly established a special—

Mr. Matthew Green: I actually want to—

Ms. Rachel Curran: Do you want to hear the answer, MP Green, or do you want to posture politically?

Mr. Matthew Green: I want to talk about something positive. I want to give you an opportunity—

Ms. Rachel Curran: I'm happy to answer your question—

Mr. Matthew Green: It's my time, Ms. Curran; it's my time. Thank you.

The Chair: Mr. Green, go ahead.

Mr. Matthew Green: I'm going to reference a New York Times article by Sheera Frenkel. It states that Israel secretly targeted U.S. lawmakers with an influence campaign on the Gaza war.

This was actually a campaign that Meta did uncover, so I want to give you the opportunity to talk a little bit about this. It began in October. It remains active on X. At its peak, it used hundreds of fake accounts on Facebook and Instagram to post pro-Israel statements. The accounts focused on U.S. lawmakers, particularly those who were Black and Democrat—and I take a specific interest in that—such as representatives like Hakeem Jeffries.

Then a further report out of NBC News said that Meta and OpenAI said that they had disrupted influence operations linked to an Israeli company. Your tech company announced that Project Stoic, which was a political marketing and business intelligence firm based in Tel Aviv, used their products nefariously to manipulate various political conversations online.

As a Canadian lawmaker, then, what assurance do I have that these same tactics, these nefarious tactics linked to this Israeli firm, weren't used to target parliamentarians such as myself?

● (1635)

Ms. Rachel Curran: Following the terrorist attacks last October 7, we quickly established a special operations centre staffed with experts, including fluent Hebrew and Arabic speakers, to closely monitor and respond to this rapidly evolving situation in real time. That allowed us to remove content that violated our community standards faster, and it served as another line of defence against misinformation. In the three days following October 7, we removed more than 795,000 pieces of content for violating these policies in Hebrew and Arabic.

The Chair: Thank you.

For the second round, we have Mr. Barrett for five minutes. Go ahead.

Mr. Michael Barrett: My question is for Ms. Patell.

YouTube chief product officer Neal Mohan, in response to Bill C-11, said the bill "has the potential to disadvantage the Canadian creators who build their businesses on our platform".

Can you tell me, Ms. Patell, about the "keep YouTube yours" campaign that was launched in response to Bill C-11?

Ms. Jeanette Patell: Of course, and thank you for the opportunity to speak to that.

As you may recall, when Bill C-11 was originally tabled, it was not intended to capture UGC, user-generated content. That was really important for our creators, because creators rely on their content being recommended to audiences who will love it, no matter where they are in the world. Think about it: Canada has about 2% of the world's population, and YouTube has a global audience of over two billion monthly logged-in users. That's the market Canadian creators care about so deeply, and when we were advocating on Bill C-11, our main message was that we wanted to ensure we were protecting the creative ecosystem these creators had built businesses on—really successful businesses—so it was not about prioritizing Canadian creators to Canadians; it needed to be about providing a level playing field for them to find their audiences all over the world. That was what we were advocating.

Mr. Michael Barrett: I know that famed Canadian creators, such as Margaret Atwood, likened this legislation to Soviet-era censorship. I'm wondering, Ms. Patell, with the bill having been enacted, do you or would you still recommend the repeal of this online censorship bill, Bill C-11, that came from the Trudeau government?

Ms. Jeanette Patell: That's a really great question.

We're obviously still in the middle of understanding how the CRTC intends to implement this measure. Our focus, regardless of the decisions of parliamentarians now and in the future, is really on protecting and preserving the ecosystem, so we will engage constructively, whether that's with the CRTC or with parliamentarians who are reviewing the future of this legislation.

Mr. Michael Barrett: I have a question for Meta about the impact of the Online News Act and the effect it's having on local journalism.

I've heard, in my community and from Canadians across the country who work in the news space, that when this law was passed, they then saw their traffic, which was coming to them for free from Facebook, hit a wall. It dropped right off. In some cases it caused outlets to lay off journalists. In some cases it caused them to close.

I'm curious about whether you have measured that impact. However, I would also like to know about the space opened up when reputable and accredited journalists, independent journalists, have left, and their space is now being filled by other actors, and also about the potential for the spread of misinformation in the place of news that was previously being sought out and shared on your platform.

● (1640)

Ms. Rachel Curran: We disagree with the contention that the space has been replaced by misinformation, MP Barrett. What it has been replaced by is content from our users' friends and families, from other pages they follow, whether those are non-governmental organizations, politicians, civic content—

Mr. Michael Barrett: Can I just interrupt?

What about the impact on local news?

Ms. Rachel Curran: We signalled to the government well in advance of removing news from our platforms that this was going to be the impact. We said, "Look, there's going to be a disproportionately negative impact on smaller digital-first publications. We would like to avoid that. We think the value transfer flows the other way. We are providing great value to publishers. Please don't scope us into the bill so that we have to remove news."

The Chair: Thank you.

Mr. Michael Barrett: Thank you for your response.

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

Mr. Anthony Housefather (Mount Royal, Lib.): Thank you.

Thank you to all of the witnesses for being here.

Ms. Curran, I have a very short question to ask you at the beginning. In your experience, Israeli companies aren't more nefarious than companies from other countries, are they?

Ms. Rachel Curran: I'll turn to my colleague, Dr. Hundley, to answer that question.

Dr. Lindsay Hundley: I would say that there is just a global rise in the number of disinformation-for-hire firms that are operating around the world. Of course, your colleague has already referenced one network that is based in Israel, but we have seen a lot of these that are based in Russia and other countries, including in the west.

Mr. Anthony Housefather: You get complaints, I assume, from both sides of the conflict that you're essentially taking one side over the other. Is that correct, Ms. Curran?

Ms. Rachel Curran: Yes, that's correct, MP Housefather.

Mr. Anthony Housefather: Thank you.

I want to come back to you, Mr. Fernández, for a second.

At the end of the last round of questioning for Ms. Khalid, you did acknowledge that you were funding the lawsuit of Mr. Strauss. You said that X would fund lawsuits of people who lost their jobs related to comments they made on the platform.

If I were a member of Parliament and made foolish comments on the platform attacking, for example, a specific ethnic group, and as a result the voters of my riding decided to not re-elect me in the next election because I said very stupid things on your platform, would I be able to get X to fund a legal challenge on that?

Mr. Wifredo Fernández: I don't believe that's in the spirit of the program.

Mr. Anthony Housefather: What if I were thrown out of my caucus? What if I were still a member of Parliament but had said very foolish things on your platform, and my party leader decided to throw me out of caucus because it embarrassed our party? Would I be able to sue to be reinstated in caucus?

Mr. Wifredo Fernández: We would welcome you to use the service to speak about your challenges and your positions.

Mr. Anthony Housefather: Okay.

Now that you have at least acknowledged that you're funding a Canadian political candidate's legal challenge, would you agree to disclose to the committee what number of political candidates in Canada you are funding legal challenges for and to provide any supporting documents related to the costs that you have incurred related to those legal challenges?

Mr. Wifredo Fernández: I'm happy to take the request back to our legal team, yes.

Mr. Anthony Housefather: Thank you very much.

Mr. de Eyre, I have a question for you and TikTok.

Am I correct that you're familiar with the Network Contagion Research Institute?

Mr. Steve de Eyre: Yes, and I saw that they testified at this committee in the spring.

Mr. Anthony Housefather: They have, exactly. Mr. Finkelstein was here at our committee on this very study.

As you know, the NCRI did a study on Chinese influence on TikTok. I'm going to read their conclusions to you. They say:

> The conclusions of our research are clear: Whether content is promoted or muted on TikTok appears to depend on whether it is aligned or opposed to the interests of the Chinese Government. As the summary data graph below illustrates, the percentages of TikTok posts out of Instagram posts are consistently range-bound for general political and pop-culture topics, but completely out-of-bounds for topics sensitive to the Chinese Government.

Those would be, for example, the Uyghurs.

I read the 26 pages of the report, and it's pretty troubling.

What is your response to the idea that TikTok is essentially muting all of the voices that are against the Chinese Communist Party?

● (1645)

Mr. Steve de Eyre: First, I absolutely disagree with the premise of the question and with the report. We have serious concerns—

Mr. Anthony Housefather: You disagree with the premise of my question? The premise of my question was simply that the report found that you were doing this. Do you disagree that the report found that you were doing this?

Mr. Steve de Eyre: We disagree with the methods and the research—

Mr. Anthony Housefather: That's not the premise of my question. The premise of my question was that the report said this; what was your opinion on the report?

Mr. Steve de Eyre: Our opinion on the report is that it used extremely flawed methods. It's misleading. There's no peer-reviewed research. Previous research done by that organization has been debunked by other outside analysts. Their method was creating fake accounts that interact with our platform in a way that normal human users would never do, so we have serious concerns about that report and their conclusions.

Mr. Anthony Housefather: I can only understand the methodology of the report from what the report says is its methodology.

The report states, "On November 13, 2023, TikTok issued a letter defending itself against accusations of anti-Israel and anti-Jewish bias"—which is something that I've actually been in discussions with TikTok on, and I agree that TikTok is doing its best to try to confront that.

The report continues, "TikTok prolifically compares relative hashtags between its platform and Instagram to buttress its argument. We have replicated TikTok's methodology"—that is in this letter of November 13, 2023—"to assess whether anomalies exist regarding the relative representation of issues on TikTok vs. Instagram."

The methodology they used in the study that you say is debunked is actually the same methodology that you used in that letter that was sent to disprove something else.

The Chair: Give a very quick response, please.

Mr. Steve de Eyre: I'd be happy to follow up. Some of my colleagues would be happy to meet with you as well to explain our concerns in more detail.

Mr. Anthony Housefather: Thank you. That would be great. Thank you.

The Chair: Thank you, Mr. Housefather and Mr. de Eyre.

[*Translation*]

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

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

I'm going to turn to Mr. de Eyre, from TikTok.

You know, there's a very important element that nobody wants to talk about. Section 7 of China's National Intelligence Law and the future of intelligence rivalries with the country states that all Chinese organizations and citizens must support, assist and co-operate with the country's intelligence services.

How does the TikTok network comply with these requirements?

[*English*]

Mr. Steve de Eyre: We are not a Chinese company. We have never provided information, Canadian user data, to the Chinese government. TikTok isn't available in China. We wouldn't provide that information if we were asked.

[*Translation*]

Mr. René Villemure: It's hard to believe.

I understand that there's ByteDance in between, the structure of the company, the board of directors with a European base, and so on.

Intelligence services in several countries are banning TikTok. There are reasons for this. It's not just because we don't like the logo. TikTok is seen as a security risk. TikTok engages in mind control, according to some.

I'm stunned by this story regarding Chinese law.

How can you reassure me?

[*English*]

Mr. Steve de Eyre: I mean, I think you just have to look at our platform and the way that millions of Canadians are using it. It's really a place for creativity and joy, for learning new things. We've just recently—

[*Translation*]

Mr. René Villemure: Excuse me for interrupting you.

Why have several governments banned TikTok, then?

[*English*]

Mr. Steve de Eyre: I mean, I focus on Canada. I can really only speak for Canada. I'd be happy to follow up if you have questions about any specific countries or regions.

[*Translation*]

Mr. René Villemure: I'd like to know why several countries have banned TikTok. We could name them, but that would be a bit long.

You must have an opinion on this.

[*English*]

Mr. Steve de Eyre: Again, I am happy to answer questions about Canada. That's my role and that's what I'm here to talk about today.

We are very proud of and confident in the work we do to protect our platform and protect user data and Canadian user data. Our moderation practices are open and transparent. As I talked about in my opening statement, we have global public community guidelines, and those are what we base our content moderation decisions on.

[*Translation*]

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

The Chair: Thank you, Mr. Villemure.

[*English*]

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

Mr. Matthew Green: Thank you very much.

My first question is for Google.

Is Google a signatory to the EU Code of Practice on Disinformation?

● (1650)

Ms. Jeanette Patell: Thank you for the opportunity to speak to this.

Yes, I believe that Google is a signatory.

Mr. Matthew Green: Thank you.

The next question is for Meta. It's the same.

Is Meta a signatory to the EU Code of Practice on Disinformation?

Ms. Rachel Curran: I don't know the answer to that question, but I would be happy to follow up.

Dr. Lindsay Hundley: I can add that we are.

Mr. Matthew Green: Thank you.

My next question is for TikTok.

TikTok, are you a signatory of the EU Code of Practice on Disinformation?

Mr. Steve de Eyre: I'm going to let my colleague Justin answer that.

Mr. Justin Erlich (Global Head of Policy Development, TikTok): Yes, we are.

Mr. Matthew Green: The last question is the same, and it is for X.

Are you a signatory to the EU Code of Practice on Disinformation?

Mr. Wifredo Fernández: No, we are not.

Mr. Matthew Green: Why?

Mr. Wifredo Fernández: We have a different approach, as I've laid out. It's around Community Notes, a decentralized approach that puts power in users' hands to add context that they would feel would be helpful, rather than a traditional fact-checking program.

Mr. Matthew Green: Who is the majority shareholder and chair of X?

Mr. Wifredo Fernández: It's Mr. Elon Musk.

Mr. Matthew Green: What percentage share does he have?

Mr. Wifredo Fernández: I don't know. I'd have to get back to you on that.

Mr. Matthew Green: Is it 80% ? Would that ring a bell, Mr. Fernández?

Mr. Wifredo Fernández: I'm not sure. I'd have to get back to you on that.

Mr. Matthew Green: Okay.

Well, would you agree that Mr. Elon Musk is the chair of X?

Mr. Wifredo Fernández: That's correct. He's chair, head of product and chief technology officer.

Mr. Matthew Green: Then he's also an executive officer of X.

Mr. Wifredo Fernández: Yes, he leads our product and engineering teams.

Mr. Matthew Green: You stated in previous testimony that X does no political funding. However, as referenced in an NBC News article title, "Elon Musk's misleading election claims have accrued 1.2 billion views on X, new analysis says", and the subtitle continues, "The nonprofit Center for Countering Digital Hate said [his] debunked claims are spreading widely and don't appear to be subject to X's Community Notes fact-checking system."

You're not signing on to the EU code and your chair has 1.2 billion views of misleading election claims as a representative of the company. What do you have to say about that?

The Chair: Go quickly.

Mr. Wifredo Fernández: No user is above Community Notes. In fact, he has received several. No one at X has the ability to place or remove a Community Note.

The Chair: Okay, Mr. Caputo, you're up for five minutes—

Mr. Matthew Green: I find that very difficult to believe. I find that, in fact, impossible to believe.

The Chair: I'm sorry, Mr. Green. Your time is up.

Mr. Caputo, go ahead for five minutes.

Mr. Frank Caputo (Kamloops—Thompson—Cariboo, CPC): Thank you, Mr. Chair.

I want to pick up on where.... The Liberals have seemingly taken a study on misinformation and are trying to spread more misinformation.

Mr. Michael Cooper: What else is new?

Mr. Frank Caputo: Mr. Fernandez, could you please take a minute to expand on the nature and role of X's legal funding program?

Mr. Wifredo Fernández: As I've shared before, the goal of the program is to support individuals whose employers have impacted their employment as a result of things they've said on the service.

Mr. Frank Caputo: To be clear, is the support provided to the person—in this case, Dr. Strauss—related solely to employment, and not political candidacy?

Mr. Wifredo Fernández: That's correct.

Mr. Frank Caputo: In this specific case, is it related solely to his forced resignation from Queen's University?

Mr. Wifredo Fernández: I don't have all the details of that particular case in front of me, but I'd be happy to follow up with more.

Mr. Frank Caputo: Thank you.

You were just talking about Community Notes, so it seems timely to reference a few.

This one is from the leader of the NDP, Jagmeet Singh, dated October 13: "Last year, Cenovus raked in $37 billion in profits. And a whopping $64 billion in 2022." There is a Community Note on that, with a link to Yahoo! Finance news.

This is from August 17: "Justin Trudeau told Canadians things would be better, instead, they've gotten worse. Families are losing their homes", and it goes on.

The Community Note says, "Justin Trudeau is in government because of a confidence and supply agreement with Jagmeet Singh."

The community note goes on. Again on August 17, Jagmeet Singh said, "Justin Trudeau built people's hopes up, only to let them down." Then he goes on to talk about rent prices, and there's a Community Note on that.

On March 18, he said:

> BREAKING
>
> The vote is in and we have forced the Liberals to:
>
> Stop selling arms to the Israeli govt,
>
> Support the ICC and ICJ,
>
> Place sanctions on extremist settlers,
>
> and much more

The Community Note says, "The motion in question does not 'force' the Liberals to do anything." It goes on.

On March 7, there's another Community Note.

Then this is one from February 27. It's a very interesting one: "80% of the grocery market is controlled by 5 corporations...Sobeys, Metro—and you guessed it, Loblaws." Then he goes on to say, "Both Liberal and Conservative Party campaigns receive donations from the three."

It's very interesting that Metro is added there, given that his brother lobbies for them.

The Community Note says, "The claim in the post is false. Corporate donations to federal political parties have been forbidden by law in Canada for over 15 years." It's similar to the Liberals saying, "assault-style weapons", which have been illegal for 40 years, and they know it.

There's another one on conflicts of interest.

What do we have? We have eight Community Notes. Have you ever seen a political leader in Canada get this many Community Notes?

● (1655)

Mr. Wifredo Fernández: I'm not sure.

All of the data related to Community Notes is publicly available and accessible. It's uploaded every single day, going back to the inception of the program. This allows researchers around the world to study the system.

Mr. Frank Caputo: Not to be outdone, the Deputy Prime Minister.... I'm looking at August 23, 2021: "Great day. My anniversary."

This is from the CBC, no less: "A video tweeted by incumbent Liberal candidate Chrystia Freeland"—the finance minister and Deputy Prime Minister now—"who served as deputy prime minister in Justin Trudeau's government, was given a label Sunday from Twitter, which marked it as 'manipulated media.' "

Have you ever seen anybody this high in government "community-noted", Mr. Fernandez?

Mr. Wifredo Fernández: Yes, I'm aware that there are, you know.... The @POTUS account in the United States has received Community Notes before.

Mr. Frank Caputo: Oh, that's interesting. Would this be on a par with things Donald Trump has stated, or is it Joe Biden? Is that where you're going?

Mr. Wifredo Fernández: The @POTUS account has received Community Notes before, yes.

Mr. Frank Caputo: That's interesting.

Okay. Let's go on now to—

The Chair: You have 30 seconds, Mr. Caputo.

Mr. Frank Caputo: I apologize. I thought I was going to have a little more time here.

This can go to Mr. Fernández or Ms. Curran.

We've heard all about Russian disinformation. We hear in Parliament that it's far-right Russian disinformation.

Isn't it true that the greatest source of disinformation, particularly when it came to the 2021 election, resulting in Mr. Kenny Chiu losing his seat, was from the PRC? Is that correct?

The Chair: We may have to come back. I'm going to give you a one-word answer—that's it.

Ms. Rachel Curran: Dr. Hundley, would you respond?

Dr. Lindsay Hundley: I cannot quantify the amount of disinformation in the 2021 election.

The Chair: You can circle back on that.

Mr. Fisher, for five minutes, go ahead.

Mr. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Thank you, Mr. Chair.

Thanks to all our witnesses for being here today and making the trip.

My questions are also—no surprise—to X.

Mr. Fernández, does X collaborate with any partners, external organizations or professional fact-checkers to address disinformation?

Mr. Wifredo Fernández: No, we do not have a traditional fact-checking program. We have developed Community Notes.

Mr. Darren Fisher: In your opening statements, you talked about the desire of X to be forthright and honest. You said—and I sort of quote you, but I might have it wrong—"a critical platform as it pertains to elections".

Your CEO, Elon Musk, has been trafficking disinformation on X as it relates to the 2024 U.S. presidential election coming up this November.

On October 4, he retweeted a false claim stating that as many as two million non-citizens had been registered to vote in Texas, Arizona and Pennsylvania. On October 19, he retweeted a post suggesting that the state's voter rolls were likely to contribute to widespread fraud. These were all debunked, and there are numerous other instances of election disinformation.

This is the CEO. Clearly your in-house fact-checking is not working.

My question to you is this: How can Canadians be sure that Elon Musk and other X employees will not spread disinformation about Canadian federal, provincial and municipal politicians, especially given that he's already opined on the platform X about Canadian affairs previously?

● (1700)

Mr. Wifredo Fernández: We have a particular policy, called the "civic integrity policy", around elections, and it is specifically focused on violations that may provide misleading information about how to participate in elections or try and intimidate people from voting. That would be applicable in a Canadian election context.

Mr. Darren Fisher: Do X users play any role in reporting the disinformation? How does that work?

Mr. Wifredo Fernández: That is where Community Notes comes into play. We have a network of 800,000 contributors around the world, including over 30,000 Canadians who have enrolled in the program. In order to become a contributor, you need an account in good standing—an account for at least six months—and a verified phone number.

Then you apply, and we onboard folks every week in a fair and randomized process. They have the ability to start rating notes for their helpfulness, whether the note contains a high-quality citation, whether it directly addresses the post's claim, whether it's easy to understand and whether it contains neutral or unbiased language.

Then we use what's called a "bridge ranking algorithm". For a post to have a Community Note, contributors who have historically disagreed on the helpfulness of Community Notes actually agree that this note is helpful, and that's when it ends up on the post.

Mr. Darren Fisher: Thank you.

I'm going to go to either Dr. Hundley or Ms. Curran.

I first got into politics in 2009, and I ran against six other people municipally. I think that the reason I won was that I was early on Facebook. None of the candidates I ran against even had a Facebook page, and I had somewhere around a thousand friends on Facebook at the time.

In your opening comments—or maybe it was Dr. Hundley who said it; I can't remember—you talked about finding millions of fake accounts and deleting them. Is that a drop in the bucket? Are there billions of fake accounts? It seems to me that an aunt of mine has had about 700 fake accounts, and they're still there.

I've been an immigration lawyer, with my picture. I've been just about every possible profile out there, and that's just me. A lot of them are still there, and when we report them, they don't come down.

I agree that if you're able to take down millions of fake accounts, that's great, but do you need more capacity? Do you still see that as a problem? Are there billions out there?

Ms. Rachel Curran: I'll let Dr. Hundley speak to the specifics of this.

I will say that we have 40,000 people working globally on safety and security, and we have invested more than $50 billion in this since 2016. We are making considerable investments.

Dr. Lindsay Hundley: What I would say is that there's not a static number of fake accounts. There are fake accounts that are created every day, and we are taking them down, often within minutes of their creation.

I think the thing that's important to understand is that when you're operating at the scale that we are, it is hard to tell when a new account is a fake account versus a new account that hasn't been aged, so we have to apply a lot of different levers to be able to distinguish between those. If we're not sure, we'll put the account into an identity checkpoint or a thing like that.

I don't think that this is an issue of capacity. It is just what it looks like when you're operating on the Internet.

The Chair: Thank you, Mr. Fisher. I can attest to that. Just last week I had a fake account taken down through Meta after my staff found it.

I thought it was your charm that propelled you to victory, not your thousand followers on a Facebook page.

Voices: Oh, oh!

The Chair: That concludes our first round. We'll now reset with six-minute rounds.

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

Mr. Michael Cooper: Thank you, Mr. Chair.

Mr. Fernández, the Trudeau government has introduced Bill C-63, known as the online harms act. It has been characterized as Orwellian by Margaret Atwood. The Atlantic has published an article in which it labelled the bill as "Canada's Extremist Attack on Free Speech". The bill has been characterized this way: "The worst assault on free speech in modern Canadian history".

Among other things, the bill will establish a so-called digital safety commission, a massive new bureaucracy of censors who will have the power to impose penalties on any person or social media service found to have permitted what Justin Trudeau deems to be "harmful content", whatever that is. The penalties will be established by the Trudeau cabinet, not Parliament.

Do you have concerns about this so-called digital safety commission and the effect it will have on the free speech of Canadians online?

● (1705)

Mr. Wifredo Fernández: We are monitoring the movement of this bill through the legislative process. Yes, we do have concerns about its impact on free speech in Canada.

Mr. Michael Cooper: I would ask Meta the same thing.

Ms. Rachel Curran: We don't actually have a position on the parts of the bill that amend the Criminal Code or the Canadian Human Rights Act, because they don't apply to us. The part of the bill that applies to social media platforms we have been supportive of, because it requires us to remove material that is already illegal and that we already remove expeditiously.

We are also supportive of Bill C-412, which is MP Rempel Garner's response to Bill C-63. We think both of those bills are good attempts to deal with harmful content online. We look forward to working with MP Rempel Garner and with Minister Virani on both those bills.

Mr. Michael Cooper: Thank you for that.

The act provides that an order of Justin Trudeau's Orwellian censorship bureaucracy could be converted into an order of the Federal Court of Canada and therefore enforced like a court order.

Mr. Fernández, can you speak to the implications of that?

Mr. Wifredo Fernández: Whether it's information requests that come through lawful legal process or removal orders that come through lawful legal process, we have a process for those to be processed and evaluated by our teams.

Mr. Michael Cooper: Yes. Well, I would just observe that the effect of that provision would be to provide that a social media provider or persons affiliated with a platform like X could be subjected to severe fines or even imprisonment for contempt of a court order on the basis of refusing to take down a post that Justin Trudeau's bureaucrats deemed to be harmful content.

Mr. Wifredo Fernández: Our goal is to maximize free speech, but within the boundaries of the law in which we operate. That's what we do here in Canada.

Mr. Michael Cooper: Okay.

I'll go back to a question I asked at the end of my last round.

The Prime Minister's department was very quick to get in touch with Facebook when it identified an article that contained disinformation about Justin Trudeau, but during the 2021 election, the Prime Minister's department, the PCO, as far as Ms. Curran was aware, made no contact with Facebook in the face of a wave of disinformation by the Beijing regime directed at Kenny Chiu and other Conservative candidates to defeat them and to help re-elect Justin Trudeau.

To the other witnesses representing the other social media platforms, were you ever contacted by the Prime Minister's department, the PCO, during the 2021 election about Beijing's disinformation efforts?

I'll ask Mr. Fernández.

Mr. Wifredo Fernández: I personally was not, no.

Mr. Michael Cooper: I don't mean you personally; I mean X.

Mr. Wifredo Fernández: I'm not sure. We would have to go back to our records and check.

Thank you.

Mr. Steve de Eyre: As I mentioned in my opening statement, TikTok worked with PCO to sign on to the declaration during the 2021 election, but I'm not aware of any specific escalations that came to TikTok during that period.

The Chair: You have about 30 seconds.

Mr. Michael Cooper: Ms. Patell, go ahead.

Ms. Jeanette Patell: I am not familiar with any requests that would have come to us in 2021 with regard to your query.

Mr. Michael Cooper: Were there any requests from the rapid response mechanism?

I'll start with Ms. Curran.

Ms. Rachel Curran: No, we did not receive any requests in 2021.

Mr. Michael Cooper: Mr. Fernández, I'll go to you next.

Mr. Wifredo Fernández: I'm not sure. We would have to go back and check.

● (1710)

Mr. Michael Cooper: Mr. de Eyre, go ahead.

Mr. Steve de Eyre: I'm not aware of any.

The Chair: Ms. Patell, go ahead.

Ms. Jeanette Patell: I'm not aware of any.

Mr. Michael Cooper: That's telling.

The Chair: Thank you, Mr. Cooper.

I believe we have Mrs. Shanahan from Châteauguay—Lacolle next.

[*Translation*]

Mrs. Brenda Shanahan (Châteauguay—Lacolle, Lib.): It will soon be Châteauguay-Les Jardins-de-Napierville.

[*English*]

The Chair: I realize that.

Go ahead for six minutes, please.

[*Translation*]

Mrs. Brenda Shanahan: Thank you very much, Mr. Chair.

The Châteauguay Facebook page is very popular with my fellow citizens. However, I find it disappointing that people put all kinds of personal information on Facebook. I'm thinking of my mother, for example, or friends or relatives. Privacy may be a little-known issue, but I find it worrying.

The question I'm going to ask Ms. Curran concerns the unanimous decision handed down by the Federal Court of Appeal on September 9, 2024.

[*English*]

The decision is called Canada (Privacy Commissioner) v. Facebook, Inc. 2024; it's FCA 140.

[*Translation*]

It overturned the Federal Court's decision and found that Facebook's practices between 2013 and 2015 had contravened the Personal Information Protection and Electronic Documents Act, because the company had failed to obtain informed consent from its users and failed to protect their personal data. The Federal Court of Appeal asked the parties to report back within 90 days of the date of the decision to indicate whether an agreement on the terms of the remedial order had been reached.

The Privacy Commissioner of Canada said he expects Facebook to now outline how it will ensure compliance with the court's decision. Meta has not indicated whether it intends to seek leave from the Supreme Court of Canada to appeal the decision.

I assume you are aware of this situation, Ms. Curran.

What does Meta intend to do about the Federal Court of Appeal's unanimous decision in the case between the Privacy Commissioner and Facebook?

[*English*]

Ms. Rachel Curran: Thank you for the question, MP Shanahan.

As I understand it, this decision is under appeal, but I don't have more detail than that, so I'll avoid commenting on the case specifically.

We have always maintained that there was no evidence that Canadians' information was shared with any external actor, including Cambridge Analytica, and the Federal Court agreed with the finding that there was insufficient evidence that Canadians' data was ever shared externally.

More importantly, in the last few years we have transformed our privacy practices at Meta and built one of the most comprehensive privacy programs in the world, and we look forward to continuing to build the services that people love and trust, with privacy at the forefront.

I won't comment any more on that decision, but I can say we agree with the decision of the Federal Court that there was no evidence that Canadians' data was ever shared with Cambridge Analytica.

[*Translation*]

Mrs. Brenda Shanahan: It's not very reassuring because doubt has really been planted among Facebook users. Everyone has seen an advertisement appear while having a private conversation with friends. For example, if the conversation is about buying a car, a car ad suddenly appears. I don't think that's very convincing.

I want to go back to the Federal Court of Appeal decision. Does Meta intend to appeal this decision? Can you give us an idea of Meta's next steps?

● (1715)

[*English*]

Ms. Rachel Curran: I can't speak to the details of that particular court case. My understanding is that a decision is being appealed, but I don't have more detail than that.

I agree with you, MP Shanahan: If people don't trust us to keep their data safe, we know they won't choose to use our products and our services.

Our business uses data to connect potential customers and users with relevant and interesting content. We can only do that if our users trust us with their data and trust us to ensure their privacy. That's why privacy is really a core priority across our company.

We have dozens of teams now, both technical and non-technical, that focus on the issue of privacy and that look at how data is protected and shared across the company—how it's collected, how it's used and how it's stored. I think it's safe to say that our privacy practices have evolved significantly in the last decade. We are confident now that privacy is really at the core of everything we do and everything we build.

[*Translation*]

The Chair: Thank you.

Mrs. Brenda Shanahan: Do I have any time left?

The Chair: No, it's over.

[*English*]

Thank you, Ms. Curran.

[*Translation*]

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

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

My question is for Mr. de Eyre, from TikTok.

In a March 15 article published by Reuters and reprinted in the Chinese edition of Forbes, we read that 60% of ByteDance shares were held by institutional groups such as Carlyle Group, General Atlantic and Susquehanna, 20% were held by employees, and the rest by Mr. Zhang Yiming, who is the founder. It is also said that, although he owns 20% of the capital, he still holds 50% of the votes in ByteDance.

What is the link with China?

[*English*]

Mr. Steve de Eyre: He is no longer the CEO or on the board of ByteDance. TikTok operates outside of China. Our CEO is Singaporean and based in Singapore. We are not a Chinese company.

As you said yourself, three of the five board members are American or French citizens.

[*Translation*]

Mr. René Villemure: Is there disinformation on TikTok?

[*English*]

Mr. Steve de Eyre: We have extensive policies against harmful misinformation and disinformation. Perhaps my colleague Justin can answer that question a bit better.

Mr. Justin Erlich: Thanks very much for the question.

We take protecting the platform and its integrity very seriously. We have a host of policies around covert influence operations and deceptive behaviour, and some of the strongest misinformation policies in the industry. We take down harmful misinformation about societal—

[*Translation*]

Mr. René Villemure: I apologize for interrupting.

Is there disinformation on TikTok, yes or no? I understand that if there is, you take care of it.

[*English*]

Mr. Steve de Eyre: I can give you some stats. We have an extensive trust and safety operation. We have tens of thousands of trust and safety employees around the world. We have extensive investments in automated moderation technology.

I can give you one stat. If you look at our transparency report, which is a public quarterly report of content that's taken down for violating our policy on authenticity and integrity—

[*Translation*]

Mr. René Villemure: Thank you, Mr. de Eyre.

I understand that you act when there is disinformation.

Have you identified certain states that are more active in terms of disinformation?

[*English*]

Mr. Steve de Eyre: Justin, do you want to take that question?

Mr. Justin Erlich: Sure. Thanks.

As I mentioned, we have teams dedicated to focusing on covert influence and foreign influence activities. They certainly identify and take down many different networks, which we share on our transparency report with monthly updates.

In terms of some of the most common activities that I think you were asking about, we've seen upticks, certainly, in Russian behaviour and networks that we have taken down in the recent past.

[*Translation*]

Mr. René Villemure: Have any states other than Russia been reported?

[*English*]

Mr. Justin Erlich: Yes, I believe we have several other states as well listed on the transparency report.

● (1720)

[*Translation*]

Mr. René Villemure: Is China one of these states?

[*English*]

Mr. Justin Erlich: It is, yes. We've identified a few networks totalling over 1,000 accounts that we've taken down.

[*Translation*]

Mr. René Villemure: Thank you very much.

You have independent specialists working to verify these things.

Who are they, briefly?

[*English*]

Mr. Justin Erlich: We attract a wide range of subject matter experts who have come from government, from academia, from civil society, and they are working on various different teams that work on developing both the policies and the detection and investigation side.

[*Translation*]

Mr. René Villemure: Thank you very much.

Ms. Hundley, I'm going to ask you a big question.

Could you tell us what cognitive warfare is?

[*English*]

Dr. Lindsay Hundley: Of course. I'm happy to.

I think that cognitive warfare or influence operations—information operations, whatever you want to call it—is a practice that dates back a long time, way before the advent of social media. It is used by governments against both their own domestic audiences and what they consider to be their foreign adversaries. There's a great diversity in the field of the types of actors who might be waging this type of activity, from political parties to governments to for-hire firms, as I mentioned earlier. That's what I guess I would start with.

If there are some more specific questions that you would like me to touch on, I'd be happy to answer those.

[*Translation*]

Mr. René Villemure: All right. I'll take you at your word.

Cognitive warfare has always existed, that's a fact. But we're seeing an increase. Do you see this increase? If so, what is it and why is it more dangerous?

[*English*]

Dr. Lindsay Hundley: I'm happy to answer that.

I think that our data would probably not necessarily confirm that it is just steadily increasing. I think that there have been fluctuations over years on how many influence operations we have found on Meta platforms, but in general, one thing we have seen is that there is a greater diversification of the actors that are in this field.

Particularly, one of the most concerning trends from our standpoint is the rise of the disinformation from for-hire firms, which essentially democratizes the tactics of foreign influence operations and also makes it much more difficult to attribute the activity to the actual benefactors who have purchased these services.

[*Translation*]

Mr. René Villemure: Thank you for your response.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Villemure.

[*English*]

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

Mr. Matthew Green: Thank you.

I do have to go back to Mr. Fernández.

Mr. Fernández, are you familiar with the Center for Countering Digital Hate?

Mr. Wifredo Fernández: Yes.

Mr. Matthew Green: Mr. Fernández, just for the record again, what's your role with X?

Mr. Wifredo Fernández: I'm a director; I head our government affairs and public policy in the United States and Canada.

Mr. Matthew Green: Then this would be directly in your purview. Are you aware of the report entitled "Social Media's Role in the UK Riots, Policy Responses and Solutions"?

Mr. Wifredo Fernández: No, I am not.

Mr. Matthew Green: I'll give you some background.

On July 29, 2024, there was a mass stabbing at a children's dance class in Southport in the United Kingdom, and three children died.

Immediately following news of the attack, false information about the attacker's identity spread on social media, alongside calls for action and violence. The next day hundreds of people gathered outside a Southport mosque and hurled petrol bombs, bricks and anti-Muslim abuse, motivated by false information spread online naming the attacker—and I won't even rename it, because I don't want to boost it anymore—and was both a Muslim and an asylum seeker.

Acts of violence and public disorder, much of it featuring anti-Muslim and anti-migrant sentiment, soon spread around the country. Posts containing the fake name were promoted by users using platform algorithms and recommended features. The Institute for Strategic Dialogue found that X featured the false name in its "trending in the U.K." promotions, suggesting it to users in the "what's happening" sidebar.

Far-right figures with millions of followers capitalized on false claims that the attacker was an asylum seeker, spreading the falsehood further into the massive bases of followers.

One platform stood out. It was yours. It was X, and the owner, whom we identified already, Mr. Elon Musk, shared false information about the situation to his 195 million followers and made a show of attacking the U.K.'s government response to the outbreak of violence. Rather than ensuring risk and illegal content were mitigated on his platform, Musk recklessly promoted the notion of an impending civil war in the U.K., Mr. Fernández, and yet your company, X, refuses to sign on to a declaration on the practice of disinformation.

What do you have to say about that, Mr. Fernández?

● (1725)

Mr. Wifredo Fernández: About what in particular, sir?

Mr. Matthew Green: I mean the fact that your platform was responsible for misinformation about the false name of a person who was identified as Muslim and an asylum seeker, which reached potentially 1.7 billion people.

Mr. Fernández, out of all of the companies here, X is the only one that refused to sign on to a code of practice on disinformation. Your owner, who is currently on the campaign trail with Donald Trump in a hyperpartisan role for X, contrary to your testimony at this committee, is responsible for this.

What do you have to say about that to the people who were targeted in the U.K., sir?

Mr. Wifredo Fernández: We have clear policies on hate, abuse and harassment. In the first half of this year, we suspended over 1.1 million accounts under these policies, removed over 2.2 million posts and actioned an additional 5.3 million posts under hate, abuse and harassment. We do take it seriously. We do act on it.

I'm happy to follow up more on—

Mr. Matthew Green: On the research relating particularly to the U.K. riots.... When I say "riots", I need you to go back and look at this. Look at the work your company is involved in on the streets, creating chaos and violence by far-right extremists.

The initial report's analysis "determined that X was a significant platform in the unrest." It reads:

> ...the X platform as accounting for roughly 50% of all public referrals of online content—double the proportion of the next largest platform. CCDH quantified the reach that far-right influencers spreading hate and false information garnered on X in the aftermath of the attack, facilitated by the platform's blue-tick promotion feature and enabled by the proprietor's decision to re-instate previously banned accounts.

In this report, sir, it was also discovered that X was "profiting from the disorder by placing advertisements alongside hate and lies". What do you have to say about that, sir?

Mr. Wifredo Fernández: Again, I'm happy to follow up with my U.K. colleagues, and we'll talk to you more about our response in that scenario.

Mr. Matthew Green: Is it an isolated incident, or do you also make a practice of profiting from online hate?

Mr. Wifredo Fernández: No, sir.

Mr. Matthew Green: Are you familiar with the Center for Countering Digital Hate's report entitled, "Hate Pays: How X accounts are exploiting the Israel-Gaza conflict to grow and profit"?

Mr. Wifredo Fernández: I'm not familiar with that particular report, but I am happy to talk about our response to the Israel-Hamas conflict.

Mr. Matthew Green: It states:

X appears to be profiting from ads served near content from hateful accounts exploiting the conflict...

Hateful accounts benefit from 'verified' perks that boost visibility of their posts

All ten accounts in our study benefited from paid-for 'blue tick' verification, which X ensures X gives their posts greater visibility from "prioritized ranking" on the platform.

Six of the hateful accounts studied have enabled X's subscription feature, enabling them to profit by charging followers to access exclusive content.

The Chair: Mr. Green, we're at six minutes now.

Mr. Matthew Green: I find it all despicable, sir—I'm going to say that—and I find the testimony not credible.

Thank you.

The Chair: Okay. Thank you.

Mr. Caputo....

That completes our first round.

We're going to go to five-minute questions and we're going to go to—

Mr. Frank Caputo: I think Mr. Barrett will be taking over now.

The Chair: We're going to go to Mr. Barrett.

Go ahead.

Mr. Michael Barrett: Mr. de Eyre, in the United States, your platform has a creator fund. Mr. Fernández talked about that aspect of his platform. Can you quickly give us some sense of what the anticipated rollout in Canada will be? Are there any plans to roll that out in Canada?

Mr. Steve de Eyre: Sure. Thanks for the question. This is something we talk a lot about with Canadian creators.

The creator fund, or the creativity fund as it's called now, is specific to the U.S. and a few other countries. We haven't rolled it out globally yet. We're always looking at ways we can continue to help creators monetize their content and earn a living from their content. There are quite a number of other ways, though, that Canadian creators are thriving and making money by using TikTok.

You have a constituent in your riding, whom I mentioned in my opening statement, Corey McMullan. He uses it for brand partnerships and to sell his own items directly to his followers. I think he has an audience of over 400,000 or 500,000 followers.

Live gifting is another major way that Canadian creators are able to monetize their platforms. They go live and receive virtual gifts.

We're constantly looking at ways we can help our community leverage their audience and earn money or even make a living through TikTok.

● (1730)

Mr. Michael Barrett: I appreciate that response.

I have a question that I'd like to put to each member of the panel, and it has to deal with the responsibility that verified users on your platforms have when it comes to the dissemination of disinformation.

Mr. Fernández, you talked about the grey check mark and the trust that users of your service can have when they recognize that the grey check mark means that this person is an elected official or a government official.

I want to read to you a post on X from October 17, 2023. Canada's foreign affairs minister posts, "Bombing a hospital is an unthinkable act, and there is no doubt that doing so is absolutely illegal." That post was viewed 2.7 million times. It's still live on your site today.

I want to juxtapose that with an ABC News story from October 18, 2023. I'm just going to read you the first paragraph:

A day after the Hamas-led Gaza Health Ministry claimed Israel had attacked the Al Ahli Arab Hospital in Gaza City, saying some 500 Palestinians had been killed, Israeli and U.S. officials, explosives experts, and President Joe Biden said Wednesday that available evidence shows the destruction was caused instead by a failed Palestinian terrorist rocket launch.

How difficult is it for your users—and also your services—to manage this when we have this type of recklessness not only from an elected official but also from the foreign affairs minister of a G7 country who is spreading what is demonstrably evidenced as fake news, false information—call it what you will?

We talk about misinformation. The chair has pointed out before that that's a clever term for when people lie. What kinds of challenges does it create when this type of actor is posting this type of misinformation?

Mr. Wifredo Fernández: At times of conflict and disasters, people come to X to find out what's happening. Often it can be challenging to understand what's happening in a conflict zone, such as the Israel-Hamas war. This is where Community Notes can be really powerful and can sometimes act faster than traditional fact-checking.

However, because so many people come to the service and there are a lot of different sources of authoritative information and important information, this is where folks can make better sense and get a more accurate picture of what's happening on the ground.

Mr. Michael Barrett: Yes, and I'll note....

I regret that I don't have time for the other platforms to engage on this question. I think I have 45 seconds left, Mr. Chair.

The Chair: You have 30 seconds.

Mr. Michael Barrett: I note that there are Community Notes that have been suggested, but an agreed-upon note has not been posted yet. However, I do think that in this case, that feature is important, because there is definitely added context, including the truth, that should have been offered by that verified user, Canada's Minister of Foreign Affairs, when posting and not taking down something that's demonstrably false.

Thanks.

The Chair: Thank you, Mr. Barrett.

I see that Mr. Bains has his headset on and that he's ready to go online there.

Go ahead, Mr. Bains, for five minutes, please.

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

Thank you to all our platform guests for joining us today.

I want to talk to Mr. Fernández regarding bots. Bots, we know, are a source of misinformation on social media platforms. Since X was sold, bots' activity on X has become worse than ever, according to experts like Timothy Graham at the Queensland University of Technology. There is an article from The Washington Post in July 2018 that reads:

> The rate of account suspensions, which Twitter confirmed to The Post, has more than doubled since October, when the company revealed under congressional pressure how Russia used fake accounts to interfere in the U.S. presidential election. Twitter suspended more than 70 million accounts in May and June, and the pace has continued in July.

However, according to your statements earlier today, Mr. Fernández, you said that X has removed 60,000 spamouflage accounts in the last year. Why is there such a discrepancy between the suspensions before Mr. Musk purchased the platform and what I referenced in 2018? Is that not a huge gap of bots still active?

● (1735)

Mr. Wifredo Fernández: One thing I would say is that compared to 2018, now, in 2024—six years later—we have a lot more activity on the service. We have more monthly and daily active users. Just in the first half of this year, as we recently disclosed in our public "Global Transparency Report", we suspended over 460 million accounts under our platform manipulation and spam, so our threat disruption teams are active and busy every day thwarting these types of campaigns.

Mr. Parm Bains: Spam would be equal to bots, or are they people actively...? Are they actual people accounts, or are you able to identify what's a bot versus an actual account?

Mr. Wifredo Fernández: It can be a mix. Our teams use different behavioural signals, when it comes to the accounts and technical signals, to determine the authenticity and whether there's coordinated and authentic behaviour. However, yes, it could be spam or individuals or a network of individuals. It really depends on the operation.

Mr. Parm Bains: That 300 million was over what time?

Mr. Wifredo Fernández: The 460 million was in the first half of 2024.

Mr. Parm Bains: To shift to Ms. Hundley, you talked about disinformation for hire. Can you expand on that, on these organizations that are now...? You said there's an increase in these organizations and in people retaining their services.

Dr. Lindsay Hundley: Yes, I would be happy to.

A disinformation-for-hire firm is simply a firm that sells services in order to conduct deceptive campaigns, generally relying on the use of fake accounts and fictitious identities. Over the years, since 2017, we have identified dozens of disinformation-for-hire firms that ran networks that violated our policies against coordinated inauthentic behaviour.

Mr. Parm Bains: What's their primary messaging? What are they focused on? What are they targeting?

I understand it must be a range of things, but can you highlight some of the key messages? Is it tropes or hitting on people's social issues that they maybe value versus devalue?

Dr. Lindsay Hundley: It really is going to depend on the benefactor who is hiring the services and what they hire them for.

I will say that recently a lot of the disinformation-for-hire firms that we see Russian-origin operations using are providing high-volume but extremely low-quality content, in which they're focused primarily on just trying to undermine support for Ukraine, both domestically and internationally. That includes trying to undermine those who support Ukraine and supporting those who are less supportive of aid to Ukraine.

That's what we've seen, primarily, from the Russian-origin disinformation-for-hire firms recently.

Mr. Parm Bains: Is it just Russia? Are you seeing it in India, for example? We saw reports: They have various media outlets also really focused on that type of campaign—maybe not—and I'm not sure how much of it is hitting your platforms.

Dr. Lindsay Hundley: Certainly the disinformation-for-hire trend is not unique to Russia. We have seen firms from a lot of different places. I don't recall, off the top of my head, whether we've seen any type of for-hire firm activity from India, but if we had, it would be as we previously disclosed.

That said, yes, I think there is also a distinction to make between disinformation-for-hire, when people are really lying about who they are and what they're doing, versus more overt influence operations that might be conducted through either overtly state-controlled media or state-aligned media.

● (1740)

The Chair: Thank you, Mr. Bains. I knew you were going to make a great point before I had to cut you off. I was going to cut you off, but then I let you go.

Thank you, Ms. Hundley.

[*Translation*]

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

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

I'll now turn to Mr. de Eyre, from TikTok.

Mr. de Eyre, aside from saying things to create a smokescreen or sidestep the issue, I'd rather you be very frank and explain the link between TikTok and China to me.

[*English*]

Mr. Steve de Eyre: TikTok is a global company. Our headquarters are in Singapore and Los Angeles. As I mentioned, three of our five board members are American or French. We store our user data in the U.S., Singapore and Malaysia.

[*Translation*]

Mr. René Villemure: So the answer is that there is no link.

[*English*]

Mr. Steve de Eyre: TikTok does not operate in China. We are not a Chinese company.

[*Translation*]

Mr. René Villemure: So there is no link between TikTok and a Chinese owner.

[*English*]

Mr. Steve de Eyre: We are owned 60% by global institutional investors, 20% by our founder and 20% by employees like me.

[*Translation*]

Mr. René Villemure: I'm interested in the 20% held by the founder, Mr. Zhang Yiming.

It's a rather solid link.

[*English*]

Mr. Steve de Eyre: Again, he's the founder. He started the company. He's no longer the CEO or the chair of the company.

[*Translation*]

Mr. René Villemure: He still holds 20% of the shares.

[*English*]

Mr. Steve de Eyre: That's correct.

[*Translation*]

Mr. René Villemure: Thank you.

Mr. Fernández, when we post a message on the platform X, why doesn't it automatically appear first on the news feed?

[*English*]

Mr. Wifredo Fernández: We have two distinct feeds. One is the "for you" feed and the other is the "following" feed. Those are two timelines.

One is powered by our recommendation algorithm, which is public. We published it last year for the world to see and give us feedback on.

The other is a reverse chronological feed of the accounts that you are following.

[*Translation*]

Mr. René Villemure: In your opinion, if it were possible to display the messages that are published on the global account of platform X in chronological order, could this help reduce the incidence of disinformation?

[*English*]

Mr. Wifredo Fernández: Again, that's a user choice and a user control that they have. When they log into the app or are on the web, they're able to select which feed and which timeline they would like to explore.

[*Translation*]

Mr. René Villemure: Do you think Twitter would benefit from offering no choice but to automatically display messages in chronological order?

The Chair: Please answer very briefly, Mr. Fernández.

[*English*]

Mr. Wifredo Fernández: You have two principal timelines that are fixed—the "for you" and the "following"—and the user has a choice of which they want to navigate to.

[*Translation*]

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

The Chair: Thank you, Mr. Villemure.

[*English*]

Mr. Green, go ahead. You have two and a half minutes.

Mr. Matthew Green: Thank you.

Many of the questions of the previous round were around the ownership of ByteDance. I did hear what I would consider to be sometimes weasel words that were used in explanations. I'll tell you why. The question wasn't about where it operates, where its servers are or who the board members are; the question was about the origins of ByteDance.

This is for the TikTok representative, Mr. de Eyre: Is it not fair to say that ByteDance, under Chinese law, does require compliance with Chinese law?

Mr. Steve de Eyre: ByteDance has entities that operate exclusively outside of China, such as TikTok. It also operates businesses inside China. TikTok does not operate in China. We do not store data—

Mr. Matthew Green: Where is ByteDance based?

Mr. Steve de Eyre: It's a global company.

Mr. Matthew Green: Are you refuting that it's based in Beijing? Is that your testimony here today?

Mr. Steve de Eyre: There are offices in China for ByteDance. As I said, it has Chinese businesses and entities that it runs. For TikTok, our headquarters are in Singapore and Los Angeles.

Mr. Matthew Green: You know, I've suspended my use of TikTok subsequent to inquiries about foreign interference that I take very seriously. I'm waiting for investigations to unfold.

I was an avid user of TikTok. I know many people who are. I give credence to what you're saying about people enjoying it. I would put to you that in fact the reason people spend so much time on TikTok is the power of the algorithms. It's the ability to profile people and continue to provide content to them that will essentially monopolize their time on the platform.

There still remains a concern, regardless of how you're answering it. You don't want to characterize ByteDance as a Chinese tech giant; I would. You don't want to say that it's Beijing-based; I would suggest that it is, yet here we are.

We have countries around the world, and I'll say specifically in the west, that are investigating the use of the algorithms that TikTok has. What do you have to say to people like me who have suspended their accounts because of the fears of the potential for foreign interference?

● (1745)

Mr. Steve de Eyre: Thanks for the question. I appreciate that.

I remember seeing your content on TikTok and I think you used it in a great way to engage with your constituents—

Mr. Matthew Green: I don't need that, Mr. de Eyre. I need you to answer the question.

The Chair: I need a quick response.

Mr. Steve de Eyre: We are absolutely committed to transparency, reporting on how we moderate content, where we store data and any government requests that we receive for data or content removal. We are transparent in posting that.

The Chair: That's wonderful. Thank you.

Thank you, Mr. Green.

We'll now go to Mr. Caputo for five minutes and Ms. Khalid for five minutes, and that'll be it.

Mr. Frank Caputo: Thank you.

Mr. de Eyre, I'm going to pick up on what my colleague Mr. Green was stating.

My recollection, and this was probably some time ago, was that government accounts were no longer able to use TikTok. Is that accurate?

Mr. Steve de Eyre: Currently there is an order from Treasury Board that says you can't use TikTok on a government-issued mobile device.

Mr. Frank Caputo: Right.

Did you have any interactions with the federal government after that occurred?

Mr. Steve de Eyre: We continue to engage with the government on policy issues. We did reach out and have some conversations with Treasury Board following that decision.

Mr. Frank Caputo: Do you recall, from your perspective, what the rationale was for the government taking that action?

Mr. Steve de Eyre: The government pointed to generalized concerns with data security. We provided the government with information about how we operate. Our public position at the time was that it didn't make Canadians safer to go after one platform. If Treasury Board, or the government, wanted to set rules for what types of apps should be on the devices of government employees, they should set a bar, and that should apply equally to all apps, not just to one app.

Mr. Frank Caputo: If I understand you correctly, do you feel as though TikTok has been singled out? Would your data security be on par with perhaps the other organizations that we have here at committee today?

Mr. Steve de Eyre: Absolutely it would, yes.

Mr. Frank Caputo: This is now about misinformation and disinformation, and we've talked a lot about Community Notes. Perhaps Ms. Hundley or Ms. Curran can help me out.

What is the equivalent of the Facebook Community Note?

Ms. Rachel Curran: We have the largest global fact-checking network of any of the online platforms. We work with over 90 different organizations around the world to fact-check content.

Mr. Frank Caputo: Let's say you fact-check something and it is false. What then?

Ms. Rachel Curran: We have a range of treatments we can apply to it. We can apply a screen that says that the content is false or partly false. It will link to an external organization's website, explaining what the fact-checking organization has found.

We can also downrank or demote that content so that it is less visible to our users. For content that is particularly problematic, we can remove it altogether. There are a range of different treatments.

Mr. Frank Caputo: Who decides what treatments a given post gets?

Ms. Rachel Curran: Our content review teams make the call on how content should be treated.

Mr. Frank Caputo: I see.

The reason I'm asking this is that Mr. de Eyre, in his opening remarks, talked about "prohibit misinformation that may cause significant harm." It's a standard of some sort. I just have a cryptic note here that I wrote to myself.

Do you recall that, Mr. de Eyre?

Mr. Steve de Eyre: Yes.

Mr. Frank Caputo: What's the threshold for "significant harm"?

Mr. Steve de Eyre: My colleague Justin could describe that for you.

Mr. Justin Erlich: We consider a wide variety of harms that we remove, including election misinformation, undermining civic integrity, medical misinformation that may lead to significant physical harm or death, or things that may cause public panic or large-scale property damages. Those are a few examples.

● (1750)

Mr. Frank Caputo: We're all parliamentarians here. We all use social media, but many of us really don't enjoy the process, because there's so much misinformation and, frankly, a lot of really mean-spirited comments. However, during an election campaign, which often is about 35-36 days in Canada, Mr. Erlich, is there a heightened awareness on TikTok's behalf with respect to these significant harms, or is it just kind of business as usual because there's just so much content to deal with?

Mr. Justin Erlich: In the midst of elections, we take our responsibility to protect the integrity of the platform incredibly seriously and we have task forces that are spun up to prepare and enforce all of our policies here.

Certainly we do scenario planning and assess various different types of things that may happen. We have dedicated teams looking to moderate and enforce content around election misinformation, hate or harassment. We also partner closely with fact-checkers whom we leverage to assess the veracity of any of the claims that may come in.

Mr. Frank Caputo: Thank you.

The Chair: Thank you, Mr. Caputo.

Ms. Khalid, before I go to you, I just want to circle back to your earlier intervention about asking for documents.

I've looked back into the book. It's clear that committees.... We've had several requests throughout the course of this meeting. I know that Mr. Housefather has made a request. There have been others that the clerk has noted. We'll follow up with whomever that request has been asked of, but it does say that we usually obtain papers simply by requesting them from their authors or owners. If the request is denied after the ask has been made, however, and the standing committee believes there are specific papers that are essential to its work, it can use the power to order the production of papers by passing a motion to that effect. Typically, the method is to ask. If we're not satisfied after that, we can move a motion.

I just wanted to make that very clear before you started.

Ms. Iqra Khalid: Chair, to clarify, I wasn't making a motion. I was just generally asking for those documents. I hope that is taken as a serious request.

The Chair: Okay. We will certainly follow up with Mr. Fernández on that. The clerk has noted the request. She will check the blues to make sure the request is accurate.

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

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

I'll direct my next couple of questions to Meta, if that's okay.

Ms. Curran, on December 20, 2023, there was a Human Rights Watch report entitled "Meta: Systemic Censorship of Palestine Content". Hundreds of Palestinian users have reported being shadow-banned or having their accounts suspended without any explanation. Does Meta acknowledge this as a form of censorship that deprives people in support of Palestinians' plight of their fundamental rights to express their opinions online?

Ms. Rachel Curran: I'm not familiar with the report. I'm sorry about that.

Look, last year we implemented a number of additional policy measures to address a spike in harmful content on our platforms. Those are still in place today. We've taken extensive steps over the past 12 months to keep people safe—

Ms. Iqra Khalid: I understand that. I would appreciate it if you could perhaps share those documents to us in written format. I would like to reclaim my time, if that's okay.

I would like to have a little bit of understanding as to how the repressing of content happens on Meta, Facebook and Instagram.

Ms. Rachel Curran: We have content policies called community standards that are published publicly. They're available at our transparency centre.

Ms. Iqra Khalid: My question really is this: How is it that if, for example, there are two sides to an issue, one side gets more repressed than another side?

Ms. Rachel Curran: Our content policies are enforced fairly across partisan divides, across political divides—

Ms. Iqra Khalid: How do you ensure that there is fairness in the marketplace of ideas that you provide to people, not just in Canada but also across the world?

Ms. Rachel Curran: That's a really good question.

Our content review teams are always looking at content decisions and making sure our policies are fair and are enforced fairly.

We also recently set up something called the Oversight Board, a really interesting model that examines the decisions we make around content. If we make decisions to remove content or to leave content up that our users disagree with, they can appeal those decisions to the independent Oversight Board. The Oversight Board will take a second look at our decisions.

● (1755)

Ms. Iqra Khalid: Where does the Oversight Board operate from?

Ms. Rachel Curran: I'd have to get back to you on that. It's an independent board. It's independent of Meta. I'll get back to you on that.

Ms. Iqra Khalid: If you could do that, please, I'd appreciate it.

In your comments to a colleague here who asked a question with respect to the Meta employees, I think you mentioned that there were 60,000 globally. How many are physically working from within Canada?

Ms. Rachel Curran: I don't know the answer to that. We have 40,000 people working in safety and security. I will get back to you on how many of those people are located in Canada.

Ms. Iqra Khalid: Thank you.

You recently cut 21,000 jobs, including in trust and safety and customer service, over multiple rounds of layoffs:

> ...[your] company dissolved a fact-checking tool that would have let news services like The Associated Press and Reuters, as well as credible experts, add comments at the top of questionable articles as a way to verify their trustworthiness. Reuters is still listed as a fact-checking partner, but an AP spokesperson said the news agency's "fact-checking agreement with Meta ended back in January."

How do you justify these cuts, especially when the year of 2024 is dubbed the election year, and people do rely on you to get a lot of the information they seek?

Ms. Rachel Curran: We have the largest global fact-checking network of any of the online platforms. I don't know about Reuters specifically, but in Canada, we use Agence France-Presse, and we're looking at bringing on another organization for the election specifically. We work with a range of organizations—over 90 now—to do independent fact-checking.

Ms. Iqra Khalid: Thank you.

If there is any additional data that you can provide that would confirm what you've said today, I'd really appreciate that.

Mr. Fernández, I'll go back to you quickly on the blue check marks and on the apparent ability now on X to be able to buy legitimacy for a number of dollars and to amplify your voice, regardless of how accurate or how truthful—or not—that voice is. It could be misinformation, disinformation, hate speech, etc., but you could purchase the blue check mark that then amplifies your voice.

Has there been any study done within X as to whether that blue check mark and the accounts associated with it have any correlation with misinformation or disinformation campaigns or with fact-checking expeditions on your platform?

The Chair: I'm going to need a quick response.

Ms. Iqra Khalid: I'm happy to take anything in writing, Chair, as you know.

The Chair: Go ahead, Mr. Fernández.

Mr. Wifredo Fernández: I'm happy to follow up on the distinction between the different check marks and on what our X Premium and X Premium+ subscriptions entail.

The Chair: Perfect. Thank you, Ms. Khalid.

I want to thank all our witnesses. I'm not going to name you all; there are just too many of you. I really appreciate the fact that you've made yourselves available to the committee for this important study.

The clerk has noted some of the requests that have come in from committee members for providing more information. She will review the blues and then get back to you.

I expect, over the course of the next coming weeks, that we are going to be providing our analysts with some drafting instructions. Once the clerk follows up with you, if you could get those answers back to the committee through the clerk as quick as possible, I would appreciate it as chair. We'll probably give you a deadline, if that's okay.

Thank you to everybody who's been here on Zoom and to everybody who's been here in person, including our technicians, clerks and analysts.

That's it. Have a great weekend, everybody.

The meeting's adjourned.