HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

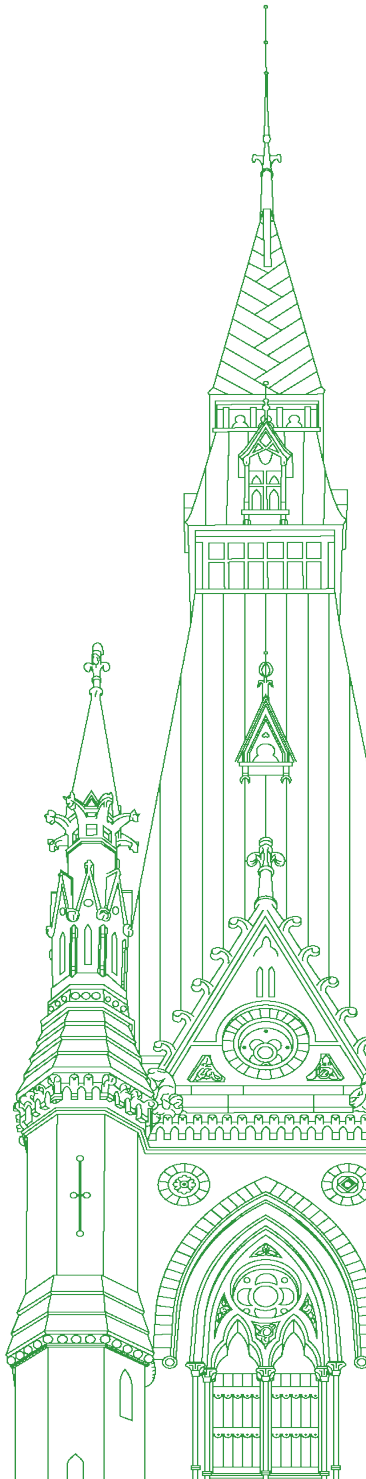
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 094

Monday, November 27, 2023



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Monday, November 27, 2023

● (1535)

[*English*]

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

I'm going to call the meeting to order.

[*Translation*]

Welcome to meeting No. 94 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[*English*]

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

[*Translation*]

Today's meeting is taking place in hybrid format, pursuant to the Standing Orders. Members are attending in person in the room and remotely using the Zoom application.

[*English*]

I just want to remind all members today that care must be taken with regard to the earpieces for interpretation. Please be mindful to not place your earpiece near the microphone, as this can result in feedback for the interpreters and may cause acoustic shock, which could in turn cause injury to our interpreters.

We have a witness in the first hour on Zoom. I will remind the committee that they have been tested and have the appropriate headwear.

I'd now like to welcome our first witness today. We have, as an individual, Dr. Anatoliy Gruzd, professor and Canada research chair in privacy-preserving digital technologies from the Toronto Metropolitan University.

Dr. Gruzd, you have up to five minutes for your opening statement.

Welcome, sir. Go ahead, please.

Dr. Anatoliy Gruzd (Professor and Canada Research Chair in Privacy-Preserving Digital Technologies, Toronto Metropolitan University, As an Individual): Thank you, Mr. Chair and committee members, for this opportunity to discuss the potential threat of foreign interference and the risks associated with the misuse of social media data.

I'm Anatoliy Gruzd, a Canada research chair and professor at Toronto Metropolitan University. I'm also a co-director of the social media lab, where I study social media's impact on society, information privacy and the spread of misinformation around conflicts such as the Russia-Ukraine war.

While my comments today are my own, they are grounded in research conducted at the social media lab and are informed by 15 years of working with various types of social media data.

As previous witnesses have testified, there are concerns that TikTok could be vulnerable to foreign interference, leading to major implications for our national security and individual privacy. However, I would like to point out that a loaded gun is different from a smoking gun. Despite its being framed as a national security threat, to date, there's still no public evidence that the Chinese government has spied on Canadians using a back door, or privileged access, to the TikTok app.

That is not to say there is nothing to worry about. There are valid concerns regarding the potential for TikTok and other platforms to be exploited by malicious actors for propaganda and radicalization. For example, Osama bin Laden's 2002 “Letter to America” recently resurfaced on TikTok and was seen by millions. However, these concerns are not limited to any one platform. Rather, they represent broader challenges to the integrity and security of our information environment.

As such, we must take a comprehensive approach to addressing these issues by compelling platforms to commit to the following: adopting the principles of privacy by design and by default, investing in expanding their trust and safety teams, and sharing data with researchers and journalists.

I'll expand each of these points.

Teaching digital literacy is important, but it's unfair to place all the responsibilities on individuals. Social media platforms are complex, and algorithms that decide what users see and don't see remain black boxes. The only true choice we have is to disconnect from social media, but it's not realistic or practical, as our own research has shown, because most Canadians have at least one social media account.

It's important to shift the focus from individual responsibility to developing strategies that compel companies to implement privacy by design and by default. Currently, it's all too common for platforms to collect more data by default than necessary.

However, even with privacy protection settings enabled, Canadians may still be vulnerable to malicious and state actors. According to a national survey that our lab released last year, half of Canadians reported encountering pro-Kremlin narratives on social media. This highlights concerns about the reach of foreign propaganda and disinformation in Canada, extending beyond a single platform.

In another example, earlier this year, Meta reported a sophisticated influence operation from China that spanned multiple platforms, including Facebook, Twitter, Telegram and YouTube. The operation tried to impersonate EU and U.S. companies, public figures and institutions, posting content that would match their identity before shifting to negative comments about Uyghur activists and critics of China.

To fight disinformation, platforms should expand their trust and safety teams, partner with fact-checking organizations and provide access to credible news content. Unfortunately, some platforms, like Meta and X, are doing the exact opposite.

To evaluate how well platforms are combatting disinformation, Canada should create an EU-style code of practice on disinformation and a transparency repository that would require large platforms to report regularly on their trust and safety activities in Canada.

To further increase transparency and oversight, Canada should mandate data access for researchers and journalists, which is essential to independently detect harmful trends. In the EU, this is achieved through the new Digital Services Act.

Currently, TikTok doesn’t provide data access to Canadian researchers, but it does so for those who reside in the U.S. and EU. Sadly, TikTok is not alone in this regard. Recently, X shut down its free data access for researchers.

In summary, while it's important to acknowledge the impact of foreign interference on social media, banning a single app may not be effective. It could also undermine trust in government, legitimize censorship and create an environment for misinformation to thrive.

A more nuanced approach should consider the various forms of information and develop strategies to address them directly, whether on TikTok or other platforms. This may involve a wider adoption of privacy by design and by default, expanding trust and safety teams in Canada and compelling platforms to share data with researchers and journalists for greater transparency and independent audit.

● (1540)

Thank you.

The Chair: Thank you, Dr. Gruzd.

We will start our six-minute round of questioning with Mr. Kurek.

Go ahead, sir. You have six minutes.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Chair.

Dr. Gruzd, thanks for being here with us today and sharing your insights with the committee. I would just mention that we have a short amount of time, the way these committees are structured, so please feel free, specifically when it comes to recommendations, to follow up with this committee if there are specific action items that you would recommend in your expertise.

You talked about TikTok and the loaded gun versus the smoking gun. I'm curious to know whether your research has included anything surrounding WeChat. I know there have been reports of a very close association between the ownership structure of WeChat and the communist state in Beijing. Has your research looked into that?

Dr. Anatoliy Gruzd: Unfortunately, WeChat, like many other messaging apps, is invisible to most researchers. The reasons are good in that these are usually private conversations. Social media researchers look at public discourse on public social media platforms. There are ways in which platforms can provide more evidence and data to researchers for public groups within those platforms. Unfortunately, we don't have this ability.

That goes to one of my recommendations: Canada should mandate research access to independent researchers for their data.

Mr. Damien Kurek: Thank you for that.

We're seeing play out before us in real time, with the conflict in Israel and Palestine and the targeting of Israelis and Gazans by the terrorist group Hamas, misinformation and disinformation. I'm wondering if you've had a chance to follow this and if you could provide some comments to the committee about the impact that would have. We've seen how the information shared online has contributed to protests that have taken place on the streets of our country.

Could you add anything to that conversation in relation to social media and the larger experience that Canadians find themselves in?

Dr. Anatoliy Gruzd: Yes. Unfortunately, social media tools, as many previous witnesses have reported, have been weaponized by various state actors and other interest groups. They are too accessible to the public in trying to shape public opinion. In some cases we hear reports about large, automated bot networks. Sometimes it's questionable, though, how effective they might be, simply because it's very hard to gain credibility on social media platforms. In some cases, like Internet research agency cases, where we actually had data provided by Twitter to researchers to dissect, investigate and do a post-mortem of their dataset, we noticed how those bot accounts would develop their credibility by posting innocent content on sites like X, later on switching to different narratives.

This is to say that state actors are using social media platforms across the board to shape our narratives and how we view them, but they also tap into our divisions and polarization. That can be done covertly or overtly. Last year, for example, the Twitter account for the Russian embassy in Ottawa was tweeting anti-LGBTQ messages on its platform. That was not hidden. It was explicit. They were speaking to the group of individuals in this country who might already have subscribed to some of those views.

That's a bit of a long answer, but I think we do see impact. Whether it's direct or indirect, a state actor is trying to impact narratives and influence opinions. Also—

● (1545)

Mr. Damien Kurek: Thanks. I hate to cut you off, but we have limited time here.

It's interesting that you would bring that up. I know that we and a number of other committees addressed foreign election interference. The use of social media was a key part of that. Certainly, if you have further comments, I would invite you to send them to the committee.

I want to go to a bit of a grey area. We had TikTok before this committee, and they said, oh, privacy is great; all they require is basic information, and their settings are set up for kids. I'm paraphrasing, obviously, but very few people read the entirety of terms and conditions. Very few people understand what information is explicitly being provided. Even fewer, I would suggest, understand how impactful the information they provide is, whether it be pictures of the front of their homes or themselves on holiday.

I'm wondering if you could provide guidance to this committee, in the minute you have left, on how to balance freedom of expression, the advancement that's taken place in the social sphere, and ensuring that Canadians' privacy and safety is safeguarded.

Dr. Anatoliy Gruzd: It goes to my point about privacy not just by design, but by default. When I installed the TikTok app on my phone just the other day, I did not even create an account and it already started tracking and sent 102 requests for information like my battery life, my device ID and such. I don't even have an account, so why do they need that information?

One way to address it is to go for platforms and marketplaces that host these types of applications, because they are the ones that approve these types of applications.

Going back to your point about long terms of service, it is a problem. One initiative that I really like is called Terms of Service; Didn't Read. It's a community-driven initiative that has been around for 10 years. They rate different terms of service for each provider, including social media platforms. They rated an E for all major social media platforms, not just TikTok. This is the lowest grade. A is the highest and E is the lowest—

The Chair: Thank you, Dr. Gruzd and Mr. Kurek.

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

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

Thank you, Mr. Gruzd, for coming in today. We really appreciate your time.

I'll start by continuing where Mr. Kurek was leading.

In the context of the Israel-Palestine war, we've seen Canadians, especially young people, being targeted for posting their views online, to the point where their employment and education are impacted. There is a kind of grouping culture online, regardless of which side of the issue they're on, and online targeting of individuals for expressing their views.

Do you think that social media companies have a responsibility to provide protection and maintenance of freedom of expression, especially for young people online?

Dr. Anatoliy Gruzd: The reason I pause is that it goes hand in hand with the type of influencer content that individuals are consuming on these platforms that would trigger or lead them to certain expressions.

One concern we've observed over the years when conducting surveys with Canadians is that more of us are turning to social media for information about conflicts like the war in Ukraine or the war in Palestine.

What if there are no credible news organizations that provide that content? The reactions that you see quite often on social media platforms are driven by the influencer content that provides the news.

When we asked TikTok users in Canada, half of them said they use the platform for news about the war between Russia and Ukraine. This is concerning, because when you go to this platform and you search for trusted news sources, the most popular ones will be CTV, Global News and CBC, according to the digital trust rating. Their number of followers is 160,000 or 150,000. They cannot compete with influencer content.

Freedom of speech is important, but it's just as important to make sure that when our citizens—Canadians—are participating in those platforms, they have access to credible information when they react to it online.

● (1550)

Ms. Iqra Khalid: Thank you for that.

You mentioned also that it's unfair to place responsibility on individuals to do their due diligence in the context of misinformation, disinformation and their own personal information that they're providing to these social media platforms.

What do you recommend? Are we talking about government regulation? Are we talking about regulation of social media platforms?

If not, is it placing or removing some of that individual responsibility from people who have to oftentimes read pages and pages of privacy agreements that they may or may not understand?

Dr. Anatoliy Gruzd: My point about not putting all the responsibility on the individuals comes from several directions. First of all, even if individuals know how to change privacy settings, many platforms will have access to their private messages. While they feel they're protected, they're actually not.

Education is important, but it doesn't necessarily mean training individuals. It's hard to change individual behaviour, but platforms can incorporate tools that can make them more efficient and effective in terms of protecting themselves.

Here are a couple of simple examples. When you go to many browsers now, they have a button when you mouse over a picture that you can use to search and find related images. It's a simple tool that I am happy to train people on, but it's already an embedded part of the platform.

We haven't talked about generative AI, but that's the next stage of this evolutionary process. How do we make sure the tools that individual users can use to detect what is real and what is authentic...? It's not a part of these platforms. It could be through digital certification or it could be through other means, but those should be part of the platforms.

The other quick point about education is that it's much more effective to institutionalize the training.

I'll give you another example. When I was preparing for this meeting, there was a test for Zoom and the instructions told me to go to incognito mode in this browser. Providing instructions is part of the process; it's part of the institution. It's much more systematic and effective.

Ms. Iqra Khalid: Thank you.

Can you perhaps walk us through how social media companies like TikTok use the information they gather? What's the role of artificial intelligence and algorithms in the use of that data as well?

Dr. Anatoliy Gruzd: The use varies widely. They are private companies making money; most of their revenue is driven by ads, clearly, and most of the data harvesting is happening for that purpose. How do they deliver eyeballs to companies and individuals who are willing to pay for those eyeballs?

A lot of this will be about collecting your interests—what you like and what you don't like—so that when the time comes, they will show you a particular ad that is attractive, and you will be a ready buyer for that. One of the concerns I have is that this type of data is being linked across platforms and through your browser history. The linkage of data is quite concerning.

You asked about artificial intelligence. Can you repeat that part?

Ms. Iqra Khalid: What's the role of artificial intelligence in that collection of data that social media platforms use, and with respect to algorithms as well?

I'll expand on that a bit. Also, how does that impact Canadians' charter rights and freedoms in how they're able to mobilize, organize or express themselves online?

The Chair: Thank you, Ms. Khalid.

You're over your time, but I am going to give Dr. Gruzd a chance to answer that.

Answer very quickly, please, if you don't mind, Dr. Gruzd.

Dr. Anatoliy Gruzd: There is a huge use of machine learning in AI to deliver content to eyeballs. Related to your point, essentially, it's concerning sometimes, when you get into echo chambers on a particular topic and that's all you see. If it's full of misinformation, driven by a recommended system, that's even more concerning. I probably don't have time, but I can expand on that later.

The Chair: Thank you, Dr. Gruzd.

[*Translation*]

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

[*English*]

Dr. Gruzd, I want to make sure that you have it on your translation.

[*Translation*]

You can go ahead, Mr. Villemure.

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

Thank you, Dr. Gruzd. I'm very pleased to be able to get some insight from someone who has as impressive a resumé as yours on this subject.

I'm going to start with a very simple question. You talked to us about the digital trust rating.

What do you think is the ethical concern of social media platforms? Is it large or small?

● (1555)

[*English*]

Dr. Anatoliy Gruzd: When you say “digital trust rating”, are you referring to that being assigned to people—users—or the platforms themselves?

[*Translation*]

Mr. René Villemure: I'll rephrase my question instead.

Do you think social media platforms have ethical concerns? To what extent? Is it a little, maybe a lot? Is it important to them?

[*English*]

Dr. Anatoliy Gruzd: That goes directly to my point about expanding their trust and safety departments, not reducing. Essentially, that's the branch of the large major social media companies that actually oversees the content moderation, so that harmful content, problematic content, will not get the audience it's seeking. Unfortunately, we hear in the news that these departments have been shrinking. Trust and safety teams are being left out, and some of the initiatives that were started a while back are being discontinued.

It is a concern. It does signal that maybe that area is not as important, because it can be easily cut when there is no need for it anymore.

[*Translation*]

Mr. René Villemure: When we look at the policies of the companies, it seems to us that they're doing the minimum required, nothing more.

What will be the impact of generating artificial intelligence on social media? What can we expect?

[*English*]

Dr. Anatoliy Gruzd: We can clearly see confusion in the future between what's authentic and what is not. Right now, we're not at that stage. In fact, in a number of studies that I've seen, when they ask human participants whether or not they recognize some of the deepfakes and other artificial intelligence-created artifacts, the humans still can recognize these.

We also see a time in the near future when it will be much harder to differentiate between generative AI content and authentic content or works. I think that's where the next battle is. We see some platforms exploring options requiring their content creators to first disclose whether any generative AI tools were used to produce that content. That's an important step.

The next step is perhaps to do some kind of digital certification or watermark on the content, so that we actually know how it was created. There is nothing wrong with generative AI, but if the content it may create is used for malicious purposes, that's of course problematic.

[*Translation*]

Mr. René Villemure: Do you think that the use of artificial intelligence on social media platforms will help make the concept of truth vaguer and, consequently, make it difficult for people to trust their interactions with the platforms in question?

[*English*]

Dr. Anatoliy Gruzd: That is exactly right. It's about the trust between the content and the particular topics, and sometimes it's just enough to create confusion. If you have a state actor that may not be able to convince us here in Canada of certain narratives, it's maybe just enough to cause some confusion.

In my research, I focus a lot on Kremlin propaganda, and we see that strategy being used a lot.

[*Translation*]

Mr. René Villemure: Have you assessed the impact of bringing QStar into the equation with social media? I understand it's early days, but do you know anything about that, or do you have any cautionary notes for us in that regard?

[*English*]

Dr. Anatoliy Gruzd: Can you expand and try to give me a bit of context?

[*Translation*]

Mr. René Villemure: This is OpenAI's most recent project, called QStar, which, again according to OpenAI, would make the use of the technology dangerous.

[*English*]

Dr. Anatoliy Gruzd: Any unregulated use of AI, perhaps, can be misused in the future. I think right now that we are in this Wild West territory, where a lot of wrong steps will be made, companies will try to innovate, and bad actors will misuse the technology.

I am glad that this committee and maybe other committees as well are trying to look into this issue. It is right now like the Wild West. It is concerning, but as any tool, it can be used for educational as well as nefarious purposes.

[*Translation*]

Mr. René Villemure: A hammer can hit a nail, but it can also kill, for sure.

There's a lot of talk about TikTok here today, but there are other social media from foreign countries that we are less familiar with. There's talk about social media from Russia, but there's also often talk about social media from India, Pakistan and Iran.

What are some of the other social media that maybe we should be looking at?

● (1600)

[*English*]

Dr. Anatoliy Gruzd: The Social Media Lab produces a report, every two years, entitled “The State of Social Media in Canada”, and we ask Canadians what platforms they use. Certainly most of the top nine platforms would be North American and U.S.-based, except TikTok is the fastest-growing platform. Around one-third of Canadians use it.

Another platform, which hasn't reached a 10% adoption rate in Canada, is Telegram. It is being adopted quite widely around the world. In fact, the rate in terms of the service rating I mentioned is, interestingly, B, so it's quite high versus E for the rest of the platforms. While it's privacy friendly or conscious of users, it's full of Kremlin propaganda discourse, so you pick your poison, unfortunately.

I would definitely keep an eye on Telegram and a lot of messaging types of apps.

I had a question earlier about WeChat and such. Those are really hard to study. Anything this committee can do to help mandate platforms to share insights on those platforms and their public groups, where most of that originates or is propagated, would be very helpful going forward.

The Chair: Thank you, Dr. Gruzd.

[*Translation*]

Thank you, Mr. Villemure.

[*English*]

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

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

I believe that in your opening remarks you mentioned the efficacy or the rationale behind targeting one platform. I think you've just dealt with some of that in response Mr. Villemure's remarks around looking at these as tools. I've heard you say multiple times that Kremlin propaganda is present.

I want to be clear. Across all regions—east, west, north, south—would you not agree that all countries, including western European countries, utilize propaganda, be they state actors or private interests, and use these platforms for nefarious purposes?

Dr. Anatoliy Gruzd: In fact, we see that happening across the board. The case I mentioned earlier that was found by Meta was quite a sophisticated information operation run through multiple platforms, not just a single platform. In fact, that content included an element whereby fake websites were created, and of course, with generative AI it is quite easy to create something like that. Essentially, you create fake content that looks like a news organization and then use social media to get eyeballs to that content, or you use targeted advertisements to get eyeballs.

I think state actors will use any tools available, and any social media platforms that are popular in Canada would be a target.

Mr. Matthew Green: It would be your assertion, of course, and logic would follow that this study should be dealing with all platforms in all regions, including all actors, those deemed both Western friendly or more authoritarian regimes that might be around the world. Would it be a safe assumption that you would support a broad look at all platforms?

Dr. Anatoliy Gruzd: I agree that we need to look at this holistically, including not just one, single platform, unless your future witnesses clearly indicate or provide evidence as to why that particular platform is a special case.

Mr. Matthew Green: I'll ask you the question.

In your opinion, does spending all of our time and focus on one platform because it happens to be from a certain part of the world hit the mark, or does that miss the mark in terms of fully understanding the risks of algorithmic interference, profiling and direction?

Dr. Anatoliy Gruzd: I think it may put emphasis on just one platform, making it sound as though other platforms are safe when, in fact, they are engaged in similar data-harvesting practices and similar data misuse, or may be used by state actors. Definitely expanding the scope and looking at the strategies used for information operation would be a much more effective angle, unless—

Mr. Matthew Green: We've spoken here quite a bit around data capitalism, surveillance capitalism and algorithmic capitalism. I want to go back to these private companies, these western ones, these American ones: Meta, Instagram and Twitter, obviously, with Elon Musk and X. Is it not true that a lot of our information profiles—click information, geographic information, our tendencies, our preferences—are collected by private companies and then sold to third parties as, really, what the product is: the commodification of the user and not the actual platform? Is that not correct?

Dr. Anatoliy Gruzd: It's been happening, and some of the measures put in place are sometimes counterintuitive or counterproductive—even the simple example of going to a website and having it ask you if you accept cookies. Well, what is my choice if I want to visit that website? There is also the example I mentioned earlier about installing the TikTok app without having an account; somebody's trying to track.... I think it's a pervasive practice across the board and across the industry.

● (1605)

Mr. Matthew Green: I want to go back to that point to be clear, though.

Regardless of where these companies originate from, when they sell to third parties there's still a likelihood—if not a high probability—that the same sensitive information that's being harvested by TikTok via ByteDance and Chinese state-owned companies could still end up in the hands of oppressive regimes to get information on their citizens—to get information on the diaspora, on dissidents, on people who might not share the same opinions as these authoritarian regimes. Is that not correct, whether it's Instagram, Facebook or X?

Dr. Anatoliy Gruzd: It's not a secret. There are a number of different data-harvesting companies that would be sharing this type of information. There is also the whole dark web that would be collecting and sharing the information that was leaked or hacked through different repositories. Unfortunately, that's the environment we're living in. That has to be taken into consideration.

Mr. Matthew Green: Is it also not true that these other actors, these other platforms, have also, in the past, provided backdoor access to messages and to information, whether it's through quasi-legal or grey-area access as it relates to perhaps not having warrants and that type of thing?

Dr. Anatoliy Gruzd: Yes. As I mentioned in my opening remarks, I think it's important to recognize different types of interference. One can imagine having a platform where a state actor has direct access—like VKontakte, which ran from Russia and was, in fact, banned in Ukraine due to this threat that was determined, that it was actually run by the state—versus the risk associated with the general data misuse practices, whether by platforms or by third parties. I know that, earlier, you and other committees were referring to Cambridge Analytica. Sometimes a third party would get access to platforms and data through legal means, such as through their developers' applications. That's another form of interference.

The Chair: Thank you, Dr. Gruzd and Mr. Green.

Dr. Gruzd, before we go to Monsieur Gourde for the second round of questioning.... You said something earlier about state actors using social media for polarization. I'm wondering if you could clarify how they would go about this. What methods would they use? Would they use the data to target individuals or groups who are sympathetic to a cause, for example? How would that occur?

Dr. Anatoliy Gruzd: Usually we're not talking about an individual like me or a colleague being targeted. It is in fact the sympathetic groups that state actors would be targeting. What happens is that they would look at political partisan views that may be aligned with their objectives. For example, when we're talking about pro-Kremlin content, that usually resonates very well with far right Conservative groups, especially in the U.S. An example would be Tucker Carlson, who was formerly on Fox News. He was channelling pro-Kremlin claims because some of those claims are aligned well with far right ideology.

Earlier I mentioned that while the state actors may create bot networks—and they did—those accounts don't have credibility; they probably will not impact individuals or groups. It's the goal of that campaign to impact somebody in power—either an influencer on TikTok or a politician running for office—and use a microphone to usefully share the same narratives and such.

The Chair: Thank you, Dr. Gruzd.

[*Translation*]

Mr. Gourde, you have five minutes.

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

I'll go back to AI. It's a very effective tool that is used in applications to speed up the transfer of information, and to study and profile us, unfortunately.

Could this tool, in the short term, become a weapon that turns against us, Canadians, or against anyone in the world who is being overly profiled? Could that in turn constitute some form of interference?

● (1610)

[*English*]

Dr. Anatoliy Gruzd: The question is a bit broad, but I'll try to contextualize it.

When we're talking specifically about generative AI tools, the concern for me, from the data privacy perspective, would be Canadians going to websites like ChatGPT. They will tag their private and personal information into the window without realizing that they are actually consenting to that data being used for future training. They don't know whether that content will be printed out or spit out in somebody else's stream. I think that would be one form of concern.

The other form of concern, of course, is social media platforms relying on AI tools to detect harmful content, just because of the scale of the problem. Earlier this year I was looking at some of the transparency report charts from Meta, showing how they removed around 65% of content automatically that was classified as harassment and bullying. There's still a significant percentage, around 35%, that users had to report for platforms to act on. From that perspective, it is important to flag some of that problematic content that they won't have enough human content moderators or fact-checkers to look at.

When we look at AI, I think we have to differentiate the kind of use case we're actually talking about.

[*Translation*]

Mr. Jacques Gourde: You gave us a good explanation of what artificial intelligence can do at the moment. Based on your explanation, it's a benevolent tool.

What do you think AI could look like on digital platforms in three, five or 10 years?

[*English*]

Dr. Anatoliy Gruzd: There will be more automation. I wonder sometimes to what extent, though. It's already writing emails for us. It's creating websites for us. There will be potential push-back. People will want to have some authentic interactions.

That's probably more of a futuristic outlook. I don't know whether you want me to continue on that line of thinking.

[*Translation*]

Mr. Jacques Gourde: We are trying to legislate on digital platforms or artificial intelligence, but in the future, I think AI will be the Achilles heel of all platforms.

Should we legislate on that, rather than on platforms?

[*English*]

Dr. Anatoliy Gruzd: The first thing, of course, is to know whether Canadian data is being used to train generative AI applications, period. That will be number one. The second is that when Canadians see content coming through social media platforms or other online news, they need to be able to differentiate between whether it's created by AI or it's not. Those are the two things I would focus on first.

[*Translation*]

Mr. Jacques Gourde: How do you think we could go about finding the most effective way of obtaining tools that would allow us to legislate or limit excesses at the international level?

[*English*]

Dr. Anatoliy Gruzd: Some of the privacy legislation tools you're considering may be effective in terms of making sure Canadians can request that their data be removed from some of those services. That could be quite effective.

The other aspects I referred to earlier, in my opening remarks.... It's about creating a repository and code of conduct for this information, in particular. Right now, it is happening and functioning. Major online platforms in the EU—these are defined as platforms with 45 million plus—report, usually every six months or so, on their activities and what they've done to stop foreign interference, country by country. We don't see any stats about it in Canada.

Related to your question about AI, when platforms take action on AI-driven content, I would like to see how much of that content.... What was the purpose?

I think that will inform our next steps.

The Chair: Thank you, Dr. Gruzd.

[*Translation*]

Thank you, Mr. Gourde.

[*English*]

Mr. Kelloway, you have five minutes. Go ahead.

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

Doctor, it's great to see you.

There have been some very great questions from all parliamentarians here.

I'm going to approach the next series of questions in a couple of ways.

First, what can average Canadians out there do to protect themselves from disinformation and misinformation? That's one.

However, you also brought up, on several occasions, what communities are doing regarding terms of service—an initiative. I'd like you to unpack that, and the EU code of ethics.

Are there three things the Government of Canada can do to bring TikTok and other social media platforms to the table in order to ensure there's less misinformation and disinformation from an economic standpoint, domestically and internationally? I think MP Green highlighted that. He has done so very effectively on many occasions.

That would be the series of questions I have, and I can unpack those as you go.

● (1615)

Dr. Anatoliy Gruzd: We have individual education and what individual Canadians can do. We have to talk about what age group we're discussing. Earlier, I heard in this committee that the focus is on the underage population, which is a quite important and vulnerable group. However, sometimes we overlook older adults and other age groups.

Frankly, education shouldn't stop, but we cannot prepare individuals for all cases. That's why I mentioned earlier that platforms should be compelled to incorporate tools that can signal whether something is potentially problematic. We had a great example during the COVID pandemic, when platforms stepped up and provided useful interventions—even simple things, such as adding a link to Health Canada when somebody talked about COVID, or flagging that some of the content in the post may not accurately relate to scientific knowledge. Those interventions are in fact helpful in reducing the spread of misinformation and disinformation. Unfortunately, lately we are seeing those initiatives being dropped completely. The things we learned from those initiatives are not applicable to other domain areas.

If we are talking specifically about the education of younger adults or teenagers, we can't just think about traditional.... We can teach those skills. Also, look at interesting interventions, such as games that essentially show.... Put them in a position of running an information operation. There are a number of interesting studies that show the effectiveness of these campaigns. They have to make themselves run such a campaign, and in that situation you actually then become more aware of things that may be coming at you in your real-life interactions.

Can you please repeat the other aspects of the question?

Mr. Mike Kelloway: Sure. I threw a few questions at you, so I would be glad to recap the next couple.

In one of your answers to a question by one of the parliamentarians here, you talked about terms of service—as I took it—as a community initiative. You can tell me if I'm wrong on that, in terms of fighting against disinformation and misinformation.

Also, can you unpack exactly why the EU code of ethics is the gold standard, or why it is helpful in combatting disinformation and misinformation?

Dr. Anatoliy Gruzd: In terms of service, the initiative I referred to is called Terms of Service; Didn't Read, ToS;DR. Essentially it's been around for 10 years. It's volunteer-run. It's supported by nonprofits. There are essentially some legal and technology experts who are trying to deconstruct each platform's terms of service, and they created a rubric. Essentially they simplify it in terms of service. You can install a browser extension. Every time you go to a platform, whether it's a social media platform or another website, if they have information about it they will show their ratings but also explain what the key concerns are in different categories. Perhaps it would be something like the fact that they have access to your private messages or they're not actually deleting your data, or other concerns. Then you can dive deeper and actually click on those concerns to read more and get to the terms of service, where it actually says so.

The reason I like this initiative is that it's an independent oversight. That leads to the second question you asked me. The initiative in the EU is called the Code of Practice on Disinformation. It started when they created this transparency centre, where large online platforms have to complete a form on which essentially they have to report back to the EU what they are actually doing to fight disinformation. They have to be very specific.

● (1620)

The Chair: Thank you.

We have two-and-a-half-minute rounds.

[*Translation*]

The Conservatives will have two and a half minutes, as will the Liberals. We will start with Mr. Villemure, who will be followed by Mr. Green.

Mr. Villemure, you have the floor.

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

You know, I'm not a Liberal.

Dr. Gruzd, what should we think of the fact that OpenAI is reviewing its terms of use by distinguishing the use that will be made of the data for business or research purposes?

Indeed, as of December 14, if we want to use ChatGPT, all our data will be likely to be used by companies.

[*English*]

Dr. Anatoliy Gruzd: This is a tricky question, because for any start-up the research used potentially will lead to business use cases. We don't know whether that dataset collected under the research umbrella would then be carried forward for other projects that are money-making for them. I think we have to imply similar principles. If it's currently PIPEDA, it should be applied equally to research data use and use for business. The only research exception I would make, essentially, is for independent vetted researchers and journalists, and that actually goes to earlier questions about what we can do to mandate access to that type of data that companies are already collecting, so that you have more independent audit of that data.

Those things can be done. The platforms will tell you that if there's a privacy or IP concern, they cannot share data with researchers. I've heard that said so many times, but in fact there are many ways to share this type of data using privacy-preserving technology, so that researchers can report it.

[*Translation*]

Mr. René Villemure: If possible, I would like you to look at the new terms of use of OpenAI and tell us what you think about it by email, because it is very worrisome, given where we are.

You mentioned a few applications earlier, including Telegram and WeChat. However, of all the messenger applications that we, as members of Parliament, use, what is the safest? We're all on WhatsApp, Telegram, and so on.

What should we be doing?

[*English*]

Dr. Anatoliy Gruzd: The safest is to disconnect from social media and the Internet, but it's not an option, as we discussed. Seriously, we really have to consider whether a messaging app is using encryption and the type of encryption that platforms don't actually have access to. That's something that should be spelled out in any messaging app. If a messaging app had access to your private messages, I would not use it, because it's very problematic.

The Chair: Thank you, Dr. Gruzd, that's sage advice.

Mr. Green, go ahead for two and a half minutes please.

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

Thank you for your testimony. I'm finding it very helpful.

We're in a unique opportunity. We have the former president of the Treasury Board here at committee now. We know that the decision to ban TikTok was one that was made by the chief information officer, who we'll have before committee. We have heard in previous testimonies from CSIS and from our Communications Security Establishment that they provided advice to the chief information officer. They wouldn't get into what the details were of their advice, but they provided advice and ultimately the decision back in February 27, I believe, was to ban this from government devices.

I would give you this opportunity, sir, and ask you this, with your subject matter expertise: If you were advising the chief information officer under this proposed ban of TikTok, what advice would you give them, and what other areas or topics might you have covered?

Dr. Anatoliy Gruzd: I heard that testimony. I think the reference was something with an unacceptable level of risk in that recommendation, and that's all we know at this point. I hope the next witness will be able to give you a bit more insight.

In the public domain, we don't have that any more than what we just said, so—

Mr. Matthew Green: I'm talking about information that you, as a subject matter expert, would provide to the CIO on the topic of social media platforms and the issues around privacy and access to information on government devices.

What information would you give them, knowing what platforms can do and where the focus should be?

Dr. Anatoliy Gruzd: If the recommendation is with regard to user data privacy, we should treat all social media platforms equally, large or small, and then we'd have to audit them in the same way. That would be my advice.

On banning one platform, as I mentioned in my opening remarks, unless there's clear evidence of some malicious acts by state actors through back doors.... Without that, by banning it, we undermine our democratic processes, and it creates a perception of politicization of this topic.

What happens if another platform...or new evidence arises that, in fact, the state actor had backdoor access? Will our citizens trust that new decision?

● (1625)

Mr. Matthew Green: That's very important.

I want to thank you for taking the time to be here. I would like to invite you, in my last 10 seconds.... If there's anything else you see from other testimony or things you might want to add some light to, you're always welcome to provide any additional comments in writing to this committee for our consideration at the report stage.

Thank you very much.

The Chair: Thank you, Mr. Green.

Thank you, Dr. Gruzd.

We'll go to Mr. Barrett for two and a half minutes.

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

Doctor, what would you say, with respect to the protection of minors and the use of social media, to the idea of all the various applications having a requirement for the companies that operate the app stores, like the Apple App Store and the Google Play store, to require an adult—ideally a parent, but an adult—approve all downloads for individuals under the age of 16 years old?

Dr. Anatoliy Gruzd: I think it's good parenting advice. In my work, I focus more on the adult population—18 plus—so I probably wouldn't be able to get into more detail on that.

My only concern is that the supervising adult might not be able to figure out whether something is malicious or not. I think there is a responsibility for those stores you're referring to to vet the platforms they host.

Mr. Michael Barrett: Yes. I think that dual obligation, of course, is for the platforming of the application by the app stores, but also for the responsible adult in a minor's life to be required to approve.

I appreciate your saying it's good parenting advice. I think it's potentially also good public policy, and that's what I'm looking to find out. With how pervasive the messages are, especially when they're sponsored by foreign state actors, malicious actors or predators, I think our children are at significant risk with the current setup and their ability to access this information, so thanks for your feedback on that.

Thanks, Chair.

The Chair: Thank you, Mr. Barrett.

Sir, did you have something you wanted to say in 20 seconds?

Dr. Anatoliy Gruzd: Yes. It's just about parents. We're assuming they're knowledgeable adults, so it goes to my point about not putting too much emphasis on individual responsibilities. Platforms have to play their part. Kids may have second devices.

The Chair: We'll go to Madame Fortier for two and a half minutes.

[*Translation*]

Hon. Mona Fortier (Ottawa—Vanier, Lib.): Thank you, Mr. Chair.

[*English*]

Thank you for being here today.

At our committee on October 18, we had David Lieber appear before us. He is the head of privacy public policy for the Americas, and he stated, “Canadian data is stored in the United States, in Singapore and in Malaysia. That's where the servers are located.”

Does this raise any flags for you? Can you comment on that statement in general?

Dr. Anatoliy Gruzd: First of all, I don't have the capacity to independently verify where the data is, in fact, stored, so that's a public statement. Knowing how interconnected online systems are, we would want to see some kind of audit of where it actually goes.

We talked about AI, and I'll explain why that's relevant. A lot of social media platforms and other online services, in order to innovate, will incorporate APIs—essentially, access to artificial intelligence applications—to improve recommendations. Essentially, there may be cases where the data is leaving servers, which is why it's sometimes hard to be definitive. Platforms like TikTok and others have partners, and they share data to enhance each other's services.

● (1630)

Hon. Mona Fortier: Because there's about a minute left, maybe you can finish your answer from the other questions you received. I know you might want to share other thoughts with us before we close.

Dr. Anatoliy Gruzd: I think we had good coverage. I think it's just to emphasize that when we talk about foreign interference, it comes in different shapes and forms.

From my perspective, it's the impact of influencers online and politicians who have platforms. They are often the largest disinformation spreaders, but it just happens sometimes that it may align with state interests of another country.

The Chair: Thank you, Madame Fortier.

Dr. Gruzd, thank you so much for appearing before our committee. I know you carried the oak today. You were the only witness. Unfortunately, we had to push a witness off because of technology issues, but I appreciate your being there by yourself today and answering the questions of the committee.

We are going to suspend for just a couple of minutes. We're going to set up for the next panel.

The meeting is suspended.

● (1630)

(Pause)

● (1635)

The Chair: I call the meeting back to order. Welcome back, everyone.

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

First of all, from the Royal Canadian Mounted Police, we have Deputy Commissioner Bryan Larkin, who is responsible for specialized policing services. Welcome, Deputy Commissioner.

We also have Brigitte Gauvin, who's the acting assistant commissioner of federal policing, national security.

Also with us today, from the Treasury Board Secretariat, is Catherine Luelo, deputy minister and chief information officer.

I understand, Deputy Commissioner Larkin, that you have an opening statement.

I'm just confirming, Ms. Luelo, that you do not have an opening statement. Is that correct?

Ms. Catherine Luelo (Deputy Minister and Chief Information Officer of Canada, Treasury Board Secretariat): I have a few comments I'd like to make, but I'll keep them brief.

The Chair: That's fine. I'll come to you after Mr. Larkin.

Go ahead, sir. You have five minutes to address the committee.

Deputy Commissioner Bryan Larkin (Deputy Commissioner, Specialized Policing Services, Royal Canadian Mounted Police): Thank you so much.

[*Translation*]

Good afternoon, Mr. Chair.

[*English*]

Hello, honourable chair and members of the committee.

My name is Bryan Larkin. I am the deputy commissioner of specialized policing. I'm joined by Assistant Commissioner Brigitte Gauvin.

First, I would like to thank all of you for the opportunity to discuss the issue. The exploitation of the personal data of Canadians by foreign actors and the commission of crimes in the digital space are of the highest priority and among the key mandates of the Royal Canadian Mounted Police.

Foreign interference affects every aspect of our lives, from the foundations of our democracy and our economic prosperity to the critical infrastructure essential to our well-being and the fundamental rights and values that define us as a society. It is a multi-layered threat, with foreign actors seeking to advance their objectives in a myriad of ways, including through state-backed harassment and intimidation of individuals and communities across Canada.

Make no mistake: Foreign governments are leveraging data harvested through popular social media platforms to profile individuals and conduct misinformation and disinformation campaigns within Canada. Among other threat activities, online data is also being used to identify and repress political dissidents who seek refuge in Canada.

Foreign interference actors are also making nefarious linkages to criminal organizations, which facilitate the commission of and profit from illicit activities such as online fraud, cyber-espionage, child exploitation and intellectual property theft.

With these considerations in mind, today we will briefly cover the RCMP's role in contributing to the protection of all Canadians from foreign interference in the cyber realm.

As Canada's national police force, the RCMP is mandated to investigate criminal activity related to serious and organized crime and national security, which includes instances of foreign interference conducted through online means. Through our national cybercrime coordination centre, the RCMP works with all law enforcement and other partners, including the Canadian anti-fraud centre, to help reduce the threat, impact and victimization from cybercrime within Canada.

In 2022, more than 30,000 reports of cyber-enabled fraud and scams had a 35% nexus to social media platforms. We also work closely with police services across our country, as they are often the first law enforcement entities to learn about state-backed cybercriminal activities targeted at Canadians.

While the RCMP is investigating cyber-threats and actors, Canadians also need to recognize the dangers as well as the impact of online activity. In particular, it's critical for all of us to understand that everything we share is collected and stored on servers. These are often located outside our national borders, where privacy rights may not have the same meaning as they do here. In essence, we leave a digital footprint across the nation.

In some foreign jurisdictions, national security laws oblige social media companies to share this personal data collected from international users with local governments. This data is then used to harass, coerce and/or threaten dissenting voices, political leadership and our diverse communities abroad, and/or to facilitate cybercriminal activities.

Youth are particularly vulnerable. They're vulnerable to cybercrime. They tend to trust in the digital environment without fully grasping the risk associated with the digital platforms. Their extensive use of social media platforms coupled with the tendency to overshare personal information makes them particularly attractive targets for cybercriminals.

Our national youth services are engaged and educate young people about online safety through collaboration with school resource officers and various organizations. Additionally, the RCMP is committed to and continues to work with our diverse communities and newcomers to provide them with information, including safety tips and how to recognize fraudulent calls and phishing scams.

NC3, which is our cyber coordination centre, and our anti-fraud centre are also engaged in the Government of Canada's "Get Cyber Safe" public awareness campaign. This aims to inform all Canadians, including youth, about cyber-threats and prevention.

The RCMP also produces operational bulletins and reporting tools for frontline police officers, strategic partners and the public, with the goal of increasing reporting on federal crimes and engaging with culturally diverse communities.

The protection of Canada and the safety of its citizens and residents are paramount to the RCMP. It will be important for all aspects of society to work together to protect against foreign interference in this space.

Thank you.

● (1640)

The Chair: Thank you, Deputy Commissioner Larkin.

Ms. Luelo, go ahead for up to five minutes, please.

Ms. Catherine Luelo: Thank you very much. I intend to take only a couple of minutes. I want to leave time for committee members to ask any questions they may have about this important topic.

Thank you for having me today virtually.

I think the deputy commissioner outlined a number of things very well. I will take just a minute to situate my role.

As the chief information officer of Canada, I am accountable for ensuring that we have clear rules and guidelines around the usage of Government of Canada devices. That's the purview through which I made the decision on TikTok.

When we're looking at making decisions around what acceptable use is in government devices, we balance a whole bunch of things, including things like privacy, what is acceptable use in business environments, and cost. All of these things go into deciding what we allow on devices.

Maybe just as a last comment, it would be my best advice that we continue to tighten our environment in terms of the use of Government of Canada devices. We have a fairly open environment, in which about 90% of Government of Canada devices allow downloads of whatever the user would like.

We have partitioned devices, some for business and some for personal use on one common device. From my experience in the private sector, that's not usual, so it would again be my advice, and the direction in which I've been moving the organization, to further tighten that environment so that we balance out the use of devices for government business and government business alone. In doing so, we are going to have a knock-on effect that I think is going to better protect the privacy of our information.

I look forward to your questions, and I will pass it back to you to allow as much time as possible for that.

Thank you.

The Chair: We appreciate that, Ms. Luelo.

We're going to start with our first six-minute round, and I have Mr. Brock for six minutes.

Go ahead, sir.

Mr. Larry Brock (Brantford—Brant, CPC): Thank you, Chair, and thank you to the witnesses for your attendance today.

With time permitting, I will circle back to the focus of this meeting, that being social media and foreign interference, but there is another pressing issue that Canadians want answers to.

Deputy Commissioner Larkin, all my questions will be directed towards you.

You'll agree that there are basic legal tenets under criminal law; namely, that ignorance of the law is no excuse and that no Canadian is above the law. That includes all members of Parliament and the Prime Minister himself.

Would you agree with that?

● (1645)

D/Commr Bryan Larkin: That's the foundation of democracy and the democratic institutions that we provide support to in enforcing the Criminal Code of Canada and other jurisdictional laws, such as provincial and/or municipal.

Mr. Larry Brock: Thank you.

Notwithstanding that no sitting prime minister has ever been criminally charged with an offence under the Criminal Code of Canada and/or convicted of a criminal offence, if the RCMP service had reasonable and probable grounds to believe that Prime Minister Justin Trudeau had committed a criminal offence, the service would charge accordingly. Isn't that correct?

Hon. Mona Fortier: Chair, on a point of order, I understand that we have guests today to discuss a topic that we have in front of us. I think we should stay on topic and not go off topic. I would appreciate it, Mr. Chair, if we could go on with the topic of the study we have right now.

The Chair: Mr. Brock is an experienced litigator, and he did say at the outset that he was going to get to where he needs to go, so I want to give him some latitude.

Generally, as you know, I give each member their time to discuss, generally, what they want. If it brings us to a point where we end up—which I expect is where Mr. Brock is going with this—then he has the floor, and he can ask whatever questions he wants.

Mr. Brock, I stopped your time. I didn't stop it right away, but I'll give you a 10-second head start, and then I'll restart your time.

Hon. Mona Fortier: Chair, can I challenge you on this?

We are talking about the relevance of the topic, and I believe that we should—

The Chair: The issue with relevance, Madame Fortier, is that it's somewhat subjective.

Mr. Brock—

Hon. Mona Fortier: Is it subjective, when we're in a committee talking about a social media study, and we're talking about the Prime Minister at this time? I think that maybe we should come back to the relevance of this topic we have in front of us as a study.

The Chair: Mr. Brock, you have the floor. I expect you're going to get to a point where you need to go.

Mr. Larry Brock: I think relevance will be established if I'm not interrupted by Liberal members.

Thank you, Chair.

The Chair: Okay, thank you.

Go ahead, Larry.

Mr. Larry Brock: Deputy Commissioner Larkin, can I have a response to that question?

If the service had reasonable and probable grounds to believe that Justin Trudeau had committed a criminal offence, the service would charge accordingly. Isn't that correct?

D/Commr Bryan Larkin: I appreciate the question.

It's obviously very hypothetical in nature. Our mandate is to investigate criminal investigations, regardless of who the target is. We have a sensitive and international investigations section that has a mandate to investigate sensitive, high-risk matters that cause significant threats to Canada's political, economic and social integrity. Again, that is left to the frontline investigators, in consultation with prosecutors, etc., to determine that. It would be hypothetical to speak to a certain scenario.

Mr. Larry Brock: I respectfully disagree with you. The mandate of every single police officer, whether it's frontline—

Hon. Mona Fortier: Chair, I have a point of order, please.

A voice: What does this have to do with social media?

The Chair: What's your point of order?

Hon. Mona Fortier: It's the same as I mentioned earlier. It's on relevance. Unfortunately, we're not discussing the topic in front of us, Chair. I challenge the fact that we should really be focusing on this study today, which is not, unfortunately, what MP Brock is doing. The relevance should be stated, and we should go back to the topic we have in front of us.

The Chair: I'm going to give him more time to establish where he's going with this. On the issue of relevance, as I said earlier, it's subjective. Mr. Brock has indicated that he's going to go to social media, and I expect that's going to happen.

Go ahead, Mr. Brock.

Mr. Larry Brock: I'm going to circle back, with respect, to Deputy Commissioner Larkin.

It's hypothetical, but I think it's a question that's easily answerable, because every single police unit in this country—and you'd agree with me—has a singular legal threshold to lay a charge as simple as mischief or shoplifting, all the way to homicide.

Does the service have reasonable and probable grounds to believe an offence has been committed? Would you agree with me, sir, that this is the legal threshold for policing in this country?

D/Commr Bryan Larkin: That would be the threshold of any criminal investigation, which is to follow the evidence to ensure we do comprehensive investigations and interviews and look at the entirety of it. That's the threshold to ensure it meets the facts and issues of the offence we're investigating.

● (1650)

Mr. Larry Brock: Thank you.

I appreciate that your service has a sensitive unit criminally investigating the Prime Minister for, potentially, obstruction of justice—

Hon. Mona Fortier: Again, Chair, I have a point of order on relevance.

The Chair: Go ahead, Madame Fortier.

Hon. Mona Fortier: Again, Chair, he said it at the beginning. MP Brock said that he would not be in line with questions on this study. I would like to bring it back to the study we have at this time. It would be appreciated if we could focus on.... As you know, we've been trying to focus on this study for a long time. We have great guests here who can answer many questions. At another time, if the MP wants to discuss another study, he can. However, today he's off on relevance with his questions.

The Chair: Thank you, Madame Fortier.

Mr. Larry Brock: Can I respond?

The Chair: On the point of order, go ahead.

Mr. Larry Brock: If Ms. Fortier or any member of the Liberal bench wishes to continue to raise a point of order on my questions before the question is even put to the witness, we are defeating the purpose for which we are here. I hear from Ms. Fortier that she wants to deal with questions surrounding social media and foreign interference. If she and her colleagues continue to interrupt me, there's going to be very little time for them to have the opportunity to deal with what they believe to be relevant questions.

I agree with you, Chair, that relevancy is a very subjective art. I stated it at the outset. With time permitting, I will be circling back to the content matter of this meeting, but I object to this constant interference by the Liberals.

Some hon. members: Oh, oh!

Mr. Larry Brock: They're laughing. Yes, you can laugh all you want, Carolyn Bennett, because it's not funny to Canadians.

The Chair: Mr. Brock, I'm going to ask you to continue.

Hon. Carolyn Bennett (Toronto—St. Paul's, Lib.): The Oscars were already given out this year.

The Chair: You said you were going to deal with the subject matter at hand. I'm going to ask, in the two minutes and 10 seconds you have left, that you go in that direction.

Thank you.

Mr. Larry Brock: Deputy Commissioner Larkin, what we were getting at before I was interrupted, now a third time, is this whole concept about a legal threshold. Notwithstanding that no prime minister has ever been charged criminally, but in relation to the RCMP investigation, which is no secret to the Liberal bench—

Hon. Mona Fortier: I have a point of order again, Mr. Chair, on relevance.

You were pretty clear that we were going to be talking about the current study. I haven't really heard, in the introduction, that we are going there. Before our guests have to answer questions, it would be great to have the relevance of this study again.

The Chair: I appreciate that, Madame Fortier. As I said at the onset, I generally give a lot of latitude in terms of lines of questioning, hoping that we end up at a point where we're dealing with the study. I expect that's where Mr. Brock is going.

I have Mr. Barrett on that point of order.

He's followed by you, Mr. Green.

Go ahead, Mr. Barrett, on the point of order.

Mr. Michael Barrett: Mr. Chair, I would expect that had we not had four interruptions in less than four minutes for Mr. Brock, or four minutes of running time—his clock had to be stopped several times—we would have the opportunity to get to where he wants to go, but he's at a disadvantage when each time the clock is stopped he restates the same question.

If he's just given the opportunity to ask his question without having to repeat it, then perhaps the fullness of what he's looking to get to would be heard by the committee, but he's not being given that opportunity.

The Chair: Thank you, Mr. Barrett.

Mr. Green, go ahead.

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

Mr. Chair, you know that I have a lot of respect for you. I think you're doing a good job in the seat there. I'm going to share with you what my concern is with what's happening right now.

My concern is that as somebody who will often use procedure.... I know that my good friend Mr. Brock will have an appreciation of this, as we spent a lot of time together on DEDC. My concern is that when filibusters arise—and they do—you will know that I often will reflect on the ruling of relevance. If what we're doing now is setting a precedent that allows for any and all topics to be debated at any and all times, that's going to affect my future interventions on relevance when it comes to filibusters.

I know that Mr. Brock has a deep respect and consideration for procedural rules, and I would ask that we get back to the study at hand, so that in future debates when I call a point of relevance you won't reflect back on today and say that anything and everything is fair game.

● (1655)

The Chair: Yes. I have generally tried to give a lot of latitude, as you know, Mr. Green, in lines of questioning, regardless of the subject matter. I happen to fundamentally believe that a member's six minutes is their six minutes. If they want to talk about rainbows and unicorns, they can do that.

Mr. Brock, I'm asking you to come back to the subject matter at hand, if you can, sir.

Mr. Larry Brock: I intend to. Thank you, Chair.

The Chair: You have the floor for one minute and 40 seconds. Go ahead.

Mr. Larry Brock: Again, Deputy Commissioner Larkin, hopefully, I can get this question out.

My social media is absolutely abuzz with concerns in regard to this particular area.

Some hon. members: Oh, oh!

Mr. Larry Brock: I can mention social media a thousand times to satisfy my Liberal colleagues, but social media is such that Canadians want to know: Is the RCMP impervious to the thought that the Prime Minister is incapable of being charged with a criminal offence?

I know this is a sensitive matter, but I asked you for a pointed response, and I'm not getting a pointed response.

If the RCMP had reasonable and probable grounds to believe that our Prime Minister, Justin Trudeau, had been involved in a criminal offence, which is your legal threshold—reasonable and probable grounds—and you consulted with the appropriate legal authorities—you consulted with the Department of Justice; you consulted with provincial and territorial Crown attorneys—if they gave you the green light that the facts and the evidence were there and that your legal threshold was met, can you advise Canadians that in that hypothetical you could charge Prime Minister Justin Trudeau with a criminal offence? Yes or no, sir.

The Chair: In 20 seconds, Deputy Commissioner....

Hon. Mona Fortier: I have a point of order on relevance again, Chair.

The Chair: I appreciate that. As I said, relevance is subjective.

Mr. Larkin, you have 20 seconds to answer that question if you want to.

D/Commr Bryan Larkin: Again, it's a hypothetical scenario, but regardless of who the suspect is, we follow the legal threshold. We're true to our oath, and we would follow the evidence of any criminal investigation. That's our mandate.

Thank you.

The Chair: Thank you, Deputy Commissioner.

Mr. Bains, go ahead for six minutes.

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

I think now you know why it's very important to do a study on misinformation and disinformation, both domestic and foreign.

A big worry for me.... I'm a father of a 15-year-old and a 12-year-old, so this is a generational risk where we're trying to find out how we can alleviate some of the concerns we all have.

My question is for the Deputy Commissioner.

I will go to you first, please. With the abundance of information that people are receiving, what are common challenges faced by law enforcement in dealing with cybercrime on social media platforms?

D/Commr Bryan Larkin: I think one of the challenges that we're seeing is the amplification of social media around involvement in criminal investigations. Generally speaking, in the majority of investigations that we now touch, whether it be a low-threshold crime, a property crime, a violent crime or exploitation, there is some form of digital entity tied to it.

The capacity for us as a national police service, the capacity for our partners and our police of jurisdiction, is that it has changed from what used to be the fundamental investigation, which was in a neighbourhood or was in a schoolyard, etc.

What we're seeing, particularly in this instance, are foreign actors who are using and amplifying social media to target Canadian citizens and/or citizens who are living from abroad in our country. That presents a significant challenge. We don't monitor social media. We obviously use it as an investigative tool or capacity, but when you look at all the various social media platforms, the reality is that the amplification of social media in criminal investigations is impacting everything we do, every single day.

Mr. Parm Bains: You don't monitor social media, but you look at it if there are complaints. Are there established protocols for information sharing between RCMP and social media companies?

I want to use an example. On X, a major in the Indian army tweeted, “It's been long time since”—he referenced a murder victim here in Canada—“was 'condemned to hell'. Time has come to eliminate a few more....” That's a major in the Indian army making that statement on Twitter, which is now known as X.

What have you established with social media companies' allowing that kind of threat?

● (1700)

D/Commr Bryan Larkin: To clarify, we don't actively monitor social media; however, we do use it as part of our investigations through open-source information. We use software that refines our searches as a part of our criminal investigations or the work we do.

Through our national cybercrime coordination centre, we have ongoing relationships with all social media platforms. We have protocols in place, particularly around child exploitation and harm to young people. Those are all things that we do.

Obviously, we are working internally with the Government of Canada on online safety and future legislation, etc. However, again, the sheer nature of this is that we work with other police jurisdictions. Information is shared with us. We obviously use that to advance investigations. We follow lawful access, production orders and/or search warrants to obtain further information from social media platforms. We have ongoing protocols with their security departments to receive and retrieve that information.

When you look at every piece of social media that we identify and track and/or use as part of our investigations, it is evidence. It has also increased the demand within our organization. The demand on policing is fairly significant.

Mr. Parm Bains: We've learned from other witnesses. We've heard about Telegram's being associated with the Kremlin and how Russia, for generations, would target a generation of people and slowly try to influence and brainwash.

Can you list any evidence of this happening with nations other than Russia trying to influence future generations of Canadians, based on some of the information you already provided in your preamble or earlier statements?

Ms. Brigitte Gauvin (Acting Assistant Commissioner, Federal Policing, National Security, Royal Canadian Mounted Police): I'll take that question, Mr. Chair.

What the national security program does is investigate criminal activities. We don't investigate social media, and we don't investigate if there's misinformation, disinformation or influence. If the criminal activities pertain to foreign interference, we absolutely will investigate that under our mandate.

As part of our investigations, we can obtain information through social media subscriber information and other information we can obtain, either through open source or via judicial authorizations. For the national security program, the criminal activity has to pertain to foreign actor interference, for example.

Mr. Parm Bains: Are there any officers assigned to monitor social media platforms?

D/Commr Bryan Larkin: No.

Mr. Parm Bains: Okay. Are any officers specially trained to navigate the platforms at any time to detect illegal activity?

D/Commr Bryan Larkin: Through the chair, yes, we certainly have officers who are trained in cybercrime and who can obviously go in and look at different information, but we don't actively use any artificial intelligence. We don't use machine learning. We don't use full-time monitoring.

I guess I'll use the cyberworld as a new neighbourhood. It's not the traditional piece where we actually have a patrol car. Trying to bring that analogy of policing to neighbourhoods, we actively investigate, but we don't actually monitor 24 hours a day, seven days a week.

The Chair: Thank you, Deputy Commissioner and Mr. Bains.

[*Translation*]

Mr. Villemure, you have six minutes.

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

Mr. Larkin, thank you very much for coming to see us today.

I always like your answers, which are clear. I'm going to follow up on what you were just talking about.

Could you tell us how you see foreign interference since the advent of social media?

Ms. Brigitte Gauvin: I'll take that one, Mr. Chair.

Thank you for your question, Mr. Villemure.

There has certainly been an increase in foreign interference in recent years. Social media is used as a vehicle for foreign entities to propel their activities.

● (1705)

[*English*]

It certainly is a trend that we're seeing. We assess that there's been a significant increase in the past several years. Definitely, social media are being used.

[*Translation*]

Mr. René Villemure: What is the impact of the growth in the use of social media on the safety of Canadians?

Ms. Brigitte Gauvin: That interference is much more difficult to detect. That's why education is important. People need to be aware that they can be monitored by foreign entities through social media. Therefore, it's important that we, the national security community and members of the RCMP in general, have engagement programs with the public, private entities and more vulnerable communities to educate people about the different ways or various mechanisms used by foreign entities to engage in interference activities.

Mr. René Villemure: People don't usually know they're at risk in a lot of cases.

I like the fact that you brought up education. The witnesses who came here felt that people needed to be educated. What I notice is that we have to ask for education.

I know this isn't directly related to your role, but how can we educate the public about a danger that they're unaware of?

Ms. Brigitte Gauvin: You raise an important point, Mr. Villemure.

Despite that fact, I think we have to continue to educate people. You can't stop educating people based on that premise. It's important to continue that education and to use different ways to do it. This is a problem that affects the government in general. There are many agencies, and we must work together to continue doing this education in order to protect Canadians.

Mr. René Villemure: I don't know who I'm directing that question to.

Have you seen an increase in the danger since the advent of AI in general or generative AI, which has been active for about a year now with the arrival of ChatGPT?

Does AI have an impact on foreign interference?

Are the dangers increased or different?

Ms. Brigitte Gauvin: The presence of artificial intelligence definitely creates big barriers.

[*English*]

It challenges the way we can conduct investigations. I'll give an example. If you're investigating a threat on social media, or if someone is making a threat through an online platform, part of our investigation is to authenticate that video. It's a very important piece of evidence. Artificial intelligence just makes it all that more difficult to be able to do that.

[*Translation*]

Mr. René Villemure: The RCMP's authority is exercised in a given jurisdiction. A video or an application may have been created in another jurisdiction, where it has no authority.

Is that a problem?

Ms. Brigitte Gauvin: We're looking at that. However, if a Canadian is threatened or the Canadian public safety or national security of Canada is threatened, that gives us the authority to act.

Mr. René Villemure: It varies according to the purpose of the threat, so to whom or to what it is intended, and not the origin of the threat as such.

Ms. Brigitte Gauvin: There you go.

Mr. René Villemure: Okay.

What does artificial intelligence bring to foreign interference? What are the examples of increased danger that this has brought?

Ms. Brigitte Gauvin: I can't give you specific examples of foreign interference caused by artificial intelligence, but I can certainly note that question and send you a more complete answer.

Mr. René Villemure: Okay, I'd love that. That's very good.

I want to come back to education, because it fascinates and worries me.

Should schools teach courses on social media or online conduct?

Ms. Brigitte Gauvin: Absolutely. That would be a great idea.

To my knowledge, educating young people about the dangers of social media is part of the school curriculum.

● (1710)

Mr. René Villemure: Okay.

What social networks should we use? We talked about TiKToK, but let's widen the spectrum. We're members of Parliament, we communicate among ourselves on so-called secure platforms. Which ones should we use?

Ms. Brigitte Gauvin: That's a good question, but I can't answer it precisely.

Mr. René Villemure: I'll come back to you, Mr. Deputy Commissioner.

D/Commr Bryan Larkin: I think that question should be addressed to Ms. Luelo, the chief information officer at the Treasury Board of Canada Secretariat.

Mr. René Villemure: I would appreciate a brief answer.

The Chair: Ms. Luelo, the floor is yours.

Could we have a very short answer, please?

[*English*]

Ms. Catherine Luelo: I think it's a very difficult question to answer, unless we understand the classification of the information you're using. It's not a simple answer. I think it's to stick within the approved set of tools that we provide to our politicians.

The Chair: Thank you.

[*Translation*]

Thank you, Mr. Villemure.

[*English*]

Mr. Green, go ahead, for six minutes.

Mr. Matthew Green: Thank you very much.

I'm going to ask a series of questions, Ms. Luelo. I'm going to ask them in a respectful way.

It's about your tenure as chief information officer. I understand—you can confirm today—there are reports that you will be ending your time as our CIO at the end of this month. Is that correct?

Ms. Catherine Luelo: It's at the end of December. That is correct.

Mr. Matthew Green: I referenced earlier that we have the former president of the Treasury Board. I know that you're here before us.

I'm going to ask you for some candour, if I could, on your time as the CIO. At any time during the decisions or consultations to ban TikTok, did you ever feel a political pressure?

Ms. Catherine Luelo: None whatsoever.

Mr. Matthew Green: How would you characterize your time as the CIO? I think you referenced it in a public statement, or somewhere it was published, as a tour of public service.

Would you consider it a mission accomplished? How would you consider the state of Canada's information security and the work that you did as CIO?

Ms. Catherine Luelo: I think the Auditor General just published a report on the state of IT modernization. I've not had a chance to read it. I think it's a good and accurate reflection of where we find ourselves in terms of our current state of technology. We've not advanced in the last 13 years. I don't think that is a win for Canadians.

In terms of my tour of service, I feel that it was always intended to be that. I hope that other private sector leaders will do the same. It is an incredible opportunity. I think that the more we can encourage public-private—

Mr. Matthew Green: I'm going to go back to the question at hand, which is the study and the decision to simply ban TikTok. You've heard...perhaps you listened in on the previous panel, so maybe you have a reference to the questions that I put to CSIS and the CSE.

Why ban just TikTok?

Ms. Catherine Luelo: TikTok was one that we started with. Since then, you'll note that we've banned WeChat and Kaspersky Lab. The direction that I provided to my team is that we will continue to tighten it. We need to continue to lessen the number of different applications that we—

Mr. Matthew Green: I think, to be clear, you stated that there should be a division between personal use for social media purposes—and let's be quite honest; it's for political purposes that are often very partisan, when it comes to elected people anyways—and our work devices.

Is it your assertion that there should be a blanket ban on all social media from government devices to help prevent any breaches of security, referencing all of the data breaches that have happened with Facebook, Instagram and other platforms? Is that the same logical conclusion you would come to as it relates to TikTok?

Ms. Catherine Luelo: I think if there's an acceptable reason for us to be using a social media platform for business purposes.... We do reach a certain type of individual through social media. I think about my 21-year-old and 24-year-old kids. They use social media, so we have to use that as a mechanism to get information to them.

As a rule, though, you have that exactly right. I would look for us to tighten up the usage of social media. There's a cost implication to its usage on mobile devices, and we have to balance data privacy, acceptable usage—

Mr. Matthew Green: What's an “acceptable risk”? I found that term interesting. What's acceptable?

Ms. Catherine Luelo: Acceptable to me would be that the value of doing the thing outweighs the risk of any potential downside.

Mr. Matthew Green: Who decides the value?

Ms. Catherine Luelo: The value could be things like, if we were doing COVID vaccination, for example, to reach out to demographics to help—

Mr. Matthew Green: With regard to COVID vaccination, then, the Department of Health could be on TikTok, distributing or publishing information, using their algorithms, to get it to as many Canadians as possible. Is that acceptable?

● (1715)

Ms. Catherine Luelo: That would be an example of acceptable. There are a number of different examples of what would be acceptable, and I think it's situation-dependent.

Mr. Matthew Green: Okay, that's fair.

I'm going to expand it a bit further. In no way at all, during your tenure—I know it's awkward, as we have the former president of Treasury Board here—did you ever feel political pressure to make decisions to go in one way or another.

Ms. Catherine Luelo: No.

To be clear, the former president of the Treasury Board was a great support, certainly in my tenure of working at the Treasury Board.

I would say, if I could offer it, that I wish we could go more quickly at things. We need to go more quickly at things. I think there is an overhead, dealing with all the different layers around government past and present, that brings us to where we are.

Mr. Matthew Green: There was something that kind of annoyed me. I'll share this with you.

I was on public accounts and government operations, and one of my first studies was an audit on our current state of technology. I remember asking the question, do we still run things on DOS? Is it that old? In some instances the answer was yes, it was actually that old.

Of course, at that time, we had a Liberal government, which said it was going to usher in this new age of openness and transparency. There was a minister for digital governance, and then, kind of unceremoniously, they just disappeared sometime in 2019.

Do you regret that? Do you think that if we had maybe kept that mandate and that whole-of-government approach—using Liberal jargon—there might have been some headway, some kind of fiscal intervention or investment by this government to get to where you wanted to go?

Ms. Catherine Luelo: I think how I would answer that is that, in my experience, digital is everybody's job. This is about delivering programs and services to Canadians, both businesses and individual citizens, and when you make it one person's job, it doesn't get done.

Mr. Matthew Green: Of course, but that's excluding your job, right? We'll still keep that one.

Ms. Catherine Luelo: I feel that you should keep the CIO of Canada, for sure.

Mr. Matthew Green: Well, I mean, you put it out there. I had to make sure we tied that up, because we have some folks who love austerity and might cut you next time they come through.

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

Mr. Barrett, for the second round, you have five minutes.

Go ahead.

Mr. Michael Barrett: Ms. Luelo, I want to pick up quickly, if I can, on your exchange with the previous questioner.

You talked about digital being everyone's responsibility, but we've seen examples of a tremendous amount of outsourcing that has happened with respect to the development of digital products in government, to the point where we're not even able to find out how many subcontractors work on a contract. Would you say that's a responsible way for the government to manage IT systems?

Ms. Catherine Luelo: I can't speak to the procurement approach—that's out of my lane—but I can tell you that there's no world in which we're going to fix this where we're not going to need to work with contractors and professional services firms.

We do not have the capacity inside of government to solve the problem by ourselves. As someone who has played that role in a number of large companies in Canada, I've always relied on a balance of our own people and firms that are well equipped to do the things to deliver digital.

Mr. Michael Barrett: With respect, I would say there's an absolute absence of balance. We have companies like GC Strategies, which are using limitless numbers of subcontractors to hide who's actually doing the work, to the point where government doesn't know. Everyone points the finger: “Well, that's not my responsibility.” Procurement is not your responsibility, and procurement say that digital is not their responsibility. At the end of the day, Canadians get stuck with a huge bill, and everyone says they're not responsible for having given them the price tag.

Chair, my next question is for the deputy commissioner.

Can the security of Canadians' data be guaranteed if the data is held on servers overseas?

I need a quick answer, if you could, sir.

D/Commr Bryan Larkin: Again, it's a challenging question, in the sense that it depends on encryption levels, actual servers, etc.

Mr. Michael Barrett: It can't be guaranteed.

D/Commr Bryan Larkin: I don't think any specific system can be guaranteed. I mean, you do all you possibly can, but it is at risk.

Mr. Michael Barrett: Does Beijing use social media to target dissidents in Canada?

Can you provide a quick answer?

Ms. Brigitte Gauvin: Mr. Chair, there are a variety of means that China and other foreign actors use to target dissidents and conduct foreign interference activities. The use of social media is definitely one of those means.

● (1720)

Mr. Michael Barrett: Did the illegal so-called police stations being run by the dictatorship in Beijing.... Was the information they were using to target the diaspora community in Canada gleaned from social media data harvesting?

Ms. Brigitte Gauvin: The alleged police stations.... It's still very much an active and ongoing investigation. Therefore, I can't provide any further details on that, as it could compromise the investigation.

Mr. Michael Barrett: Please provide a very quick answer: Do you think it's a good idea, Deputy Commissioner, to have a requirement for app stores like the Apple App Store and the Google Play store to have a responsible adult—a parent—approve the download of all applications for individuals under the age of 16 years old? Do you think that would be a good practice and limit the exploitation and exposure of children?

D/Commr Bryan Larkin: I think it would be a progressive dialogue from a policy perspective, yes.

Mr. Michael Barrett: Thank you.

I cede my remaining time to Mr. Gourde.

[*Translation*]

The Chair: You have a minute and a half.

Mr. Jacques Gourde: Thank you.

Given the foreign interference that occurred during the 2019 and 2021 elections, will you have the mandate to intervene if there are cases of obvious or demonstrated foreign interference during the next election period?

Ms. Brigitte Gauvin: I'll take that one, Mr. Chair.

The RCMP didn't have an investigation under way during the 2019 and 2021 elections. If, in a future election, there are allegations of foreign interference, we can intervene on an ad hoc or on request basis.

We share this mandate with the Office of the Commissioner of Canada Elections. The RCMP, as part of its national security program, certainly has a mandate to do that.

Mr. Jacques Gourde: I'd like to talk about the time it takes you to intervene, because an election lasts only 35 days, which is very short. However, it's often a matter of hours. If it takes two months, it's too late. Is it possible to do it in two days?

Ms. Brigitte Gauvin: Are you talking about an investigation?

Mr. Jacques Gourde: I'm talking about the investigation to determine whether it's necessary to intervene. It has to be fast, and it has to be efficient.

Ms. Brigitte Gauvin: With respect to our actions, we investigate all allegations of criminal activity that we receive. As soon as we receive them, a file is opened and a team is assigned to it.

Mr. Jacques Gourde: What can you do to intervene? Will you disclose that there was interference in such and such a riding and that such and such a message was sent?

It has to be known in real time.

The Chair: Give a short answer, please.

Ms. Brigitte Gauvin: We have a variety of ways to warn people. Of course, there are investigative techniques that we can't disclose, since this is sensitive information, but communication with society and the people concerned, among others, is a way of fighting foreign interference.

The Chair: Thank you.

[*English*]

Ms. Khalid, go ahead for five minutes.

Ms. Iqra Khalid: Thank you very much, Mr. Chair, and thank you to the witnesses for being here today.

Perhaps I will start with Deputy Commissioner Larkin.

You mentioned earlier that the majority of the work you do with respect to this issue specifically is more investigative and reactive.

Do you think the RCMP should be taking a more proactive approach to the protection of information, especially on social media platforms?

D/Commr Bryan Larkin: It's very challenging for us as an organization to react to the amplification and impact of social media. Much of our work is reactive in nature.

Through our NC3, we are very proactive in attempting to work on preventive measures—education through the anti-fraud centre. Our national child exploitation unit does a series of educational pieces around protecting vulnerable individuals. However, we would be greatly assisted by legislation that supports other parameters in protecting vulnerable individuals, and in modernization. One challenge is that we're evolving—it's ongoing—in terms of the impact of social media on our society.

Again, although we would like to transition to this, the reality is that our capacity is limited.

Ms. Iqra Khalid: Thank you for that.

To pick up on potential legislation, do you think it would be helpful for offices like yours, the RCMP and other law enforcement to be able to rely on a national registry that has a list of all artificial intelligence applications or the use thereof by social media platforms for you to rely on to know what is out there? I think that might be half the challenge of trying to protect vulnerable communities, if you don't know exactly what kinds of applications or artificial intelligence systems are being used by social media platforms, for example.

● (1725)

D/Commr Bryan Larkin: These are progressive policy discussions and dialogues that should occur, as they would actually inform the greater public and those who use social media. In short, yes, I think we need to consistently evolve as a nation around how we continue to manage social media and the impact on all of our institutions, but also the impact on our daily life. Yes, in short, again, these are modern, progressive policy discussions that should be occurring.

Ms. Iqra Khalid: Thank you very much.

I'll ask the chief information officer the same question, if that's okay.

Do you think a national registry that catalogues all artificial intelligence applications and their uses in Canada would be helpful in ensuring the privacy and safety of Canadians?

Ms. Catherine Luelo: I will defer to the deputy commissioner on that in terms of external, but from an internal perspective, certainly, the guidance we're providing inside government is to ensure we have transparency around where we're using AI and, certainly, from a generative AI perspective, doing the same. We just issued some guidance around that.

Ms. Iqra Khalid: Thank you.

Chair, with my remaining time, I would like to move a motion, if that's okay.

I'll read it out:

> That, notwithstanding any previously adopted motion of this committee, in relation to the committee's social media and foreign entity study:
>
> (a) That the committee send invites to any witnesses who have not yet been invited and reinvite, as necessary, witnesses from whom we are still waiting for an answer to appear;
>
> (b) That the committee issue a summons for the following witnesses to appear as soon as possible:
>
> (i) Garrick Tiplady, VP Global Business Group and Country Director, Meta Canada;
>
> (ii) Sabrina Geremia, VP and Country Managing Director, Google Canada;
>
> (iii) Paul Burns, Managing Director, Twitter Canada;
>
> (iv) Shou Zi Chew, CEO, TikTok;
>
> (c) That the committee dedicate as many meetings as possible to completing the witness testimony, and that the committee not hear from any witnesses on studies related to another topic until the committee is satisfied that all witnesses in (a) and (b) have testified; that the committee set a deadline of Tuesday, November 28 at 12:00 p.m. EST to submit new witnesses to the clerk of the committee—

And, very importantly, Chair:

> —that all witnesses be given reasonable notice to prepare and attend committee meetings.

I believe a copy of this motion has been sent to the clerk.

Mr. Michael Barrett: Can we suspend, Chair?

The Chair: We're going to suspend for a minute. I need to consult the clerk.

● (1725)

_____(Pause)_____

● (1730)

The Chair: The meeting is back in session.

There's been a motion moved by Ms. Khalid. All members of the committee should have that motion. It's in relation to the current study, so it is an admissible motion.

Before we get into debate—and I see your hand, Mr. Kurek—Deputy Commissioner Larkin and Madame Gauvin, I'm going to release you at this point, if you don't mind. I want to say thank you for appearing before the committee today and providing valuable information.

Ms. Luelo, I'm going to release you as well.

It's not as easy for me. You have to click "cancel" or "leave meeting", but I do appreciate all of you for being here today. Thank you.

Ms. Catherine Luelo: Thank you for the opportunity.

The Chair: You can speak to your motion, Ms. Khalid, and then I'm going to go to Mr. Kurek.

Ms. Iqra Khalid: Thank you.

I hope members have had the opportunity to read the text of the motion. I just want to clarify that the objective of this motion is for us to wrap up this study. We started this in October. It's now December. We haven't really got through the spirit of the initial motion that passed this.

I want to clarify that point (c) doesn't mean that this study will go on forever. If it takes two meetings or three meetings to get through the witnesses we have before us and be able to write an effective report, that's what I'm looking for, Chair. I really want us to move forward with this study as early as possible, so that we can present and table a report in the House and find some concrete solutions to the very important issues we're discussing.

Again, I will reiterate that this does not mean I intend for this study to go on forever.

The Chair: Thank you, Ms. Khalid.

For the benefit of the committee, I'm going to let you know that we have resources until about 5:45. We've had a few delays. The clerk has advised me of that.

On the motion, Mr. Kurek, you have the floor.

Mr. Damien Kurek: Thanks very much, Chair.

I find it interesting. Reading this motion, it shows that a filibuster by any other name.... I've not, in my experience—now having been elected for a number of years and having spent a fair amount of time at this committee and others—seen a motion that says "as many meetings as possible to complete the witness testimony".

Certainly, I understand there are some topics of discussion that this committee has undertaken that make the government uncomfortable, but I think it's a wide-reaching motion that basically says this may never end. I think it is concerning and certainly indicative of an ulterior motive.

That's not to diminish the importance of the subject at hand, but I think, Chair, we've had the conversation before that we can't walk and chew gum at the same time.

I would, just if I could.... I don't want to give up my time, Chair, but I know this committee has spent some time working out a work plan. I understand that the next two meetings are particularly seized with this, so in terms of information for the committee, I believe it would be relevant...and then I have some further comments, so I'll certainly continue on that.

However, Chair, I'm wondering if you could direct the clerk or the analysts to share the specifics of what the work plan includes, specifically related to the next two meetings, and then I'll have a couple of further comments.

● (1735)

The Chair: I appreciate the question, Mr. Kurek. You'll still have the floor when we return.

We have witnesses for the 29th. We've been working on witnesses for December 4. We actually have the notice of meeting ready to go out. They would be Mr. Caraway, who, unfortunately, had some technical issues; Dr. Emily Laidlaw, associate professor and Canada research chair in cybersecurity law from the University of Calgary; Mr. Matt Malone is scheduled to appear; and from the Dais, we have Sam Andrey, managing director, and Joe Masoodi, senior policy analyst.

I'm going to refer to the clerk to speak specifically about the meeting on December 4.

Do we have witnesses at this point for December 4, Madam Clerk, or are we still waiting to hear?

The Clerk of the Committee (Ms. Nancy Vohl): I still have to send invitations and confirmations. Also, I would like direction from the committee—

The Chair: Okay. Of course, on December 11, we've agreed through our work plan—perhaps the analyst can expand on this—to have the RCMP commissioner here in relation to the motion that was passed by the committee as it relates to SNC-Lavalin.

Is there anything you would like to add?

Ms. Alexandra Savoie (Committee Researcher): I was just going to say, as Nancy just said, we're looking for instructions, whether it's through Ms. Khalid's motion...because, technically, as you've noticed, some witnesses have declined the invitation. However, in terms of the work plan that was circulated, it is at the end of the work plan. That's why we need instructions as to whom we invite next.

The Chair: That's the answer to that question, Mr. Kurek.

You still have the floor. Go ahead.

Mr. Damien Kurek: Thanks, Mr. Chair.

It's very telling, I think—and this committee is seized with what is an important discussion surrounding social media and its impact on Canada and Canadian young people—that passing the motion as it's written, Mr. Chair, would effectively override the work plan that has, in its future, the commissioner of the RCMP coming to appear regarding SNC-Lavalin. I think it's pretty clear that there is an ulterior motive.

As well, I would note that, with the witnesses to appear, they have Meta—Facebook. There's a vice-president for Google and a managing director of Twitter Canada. However, then they ask the CEO of TikTok. For consistency, to ask executive members of those organizations to come, I think, would also be very reasonable when having this discussion.

That point aside, Mr. Chair, I would move an amendment to Ms. Khalid's motion. It would simply be that (c) be deleted from the motion.

Ms. Iqra Khalid: Do you mean (c) in its entirety?

Mr. Damien Kurek: Yes.

The Chair: The amendment from Mr. Kurek to the motion moved by Ms. Khalid is to remove paragraph (c).

Is there any discussion on the amendment? Please keep in mind that we have until 5:45.

Go ahead, Mr. Barrett.

Mr. Michael Barrett: Mr. Chair, I guess it would be helpful to know the number of witnesses who have declined to appear. That would be important information. If you could provide that information, then I would like to speak further to the amendment.

The Chair: I'm just going to go back to last week. I believe the clerk sent out a list of where we were with the witnesses.

Was that sent to all members of the committee?

The Clerk: It was requested by Ms. Fortier, but it was not sent to everybody.

The Chair: It was requested by Ms. Fortier.

The Clerk: I can send it.

The Chair: We can certainly send that out to you, if you're looking for information on that now. Would you prefer that we send that out to you, Mr. Barrett, or...?

Mr. Michael Barrett: It would be well received, but the number of witnesses, if you could....

The Chair: If we can do rough math here....

Mr. Michael Barrett: That would be great.

● (1740)

The Chair: Okay, Madam Clerk, if you want to....

The Clerk: You would like to know, approximately, how many people have declined.

The Chair: Yes. How many people have declined?

The Clerk: Nine have declined, but some of them are double, because some of them were suggested by both the Conservatives and the Liberals.

The Chair: Nine in total have declined of those who were asked. Some of them were on multiple parties' lists.

Can you just clarify what that yellow line is there?

The Clerk: Those are the people we've not been able to get in touch with.

The Chair: Okay, we are waiting for an answer.

We have roughly, by my count, about five or six from whom we haven't heard back at this point. Nine have refused, have said “no”, and we're still waiting for a response from, roughly, five.

Ms. Iqra Khalid: I'll just clarify. Some of those nine are listed in my motion.

The Chair: The clerk just reminded me that some of them were not invited at this point because they were not part of the work plan that was approved by the committee.

I'll just remind members, as well, that the reason the RCMP commissioner is coming on December 11 is that he made himself available to appear on that date. We had agreed to start the SNC study after the social media study, but the RCMP commissioner said that he was available on December 11, so that's why we agreed to have him come on that day. Obviously, we have to accommodate his schedule, too.

Mr. Barrett.

Mr. Michael Barrett: Being mindful of the time, Mr. Chair, I would be interested to know if you sought, from committee, consensus to action item (a) of Ms. Khalid's motion—just on consensus—and to fit those folks in based on the work plan that was approved by the subcommittee. If you have time to do that in the remaining three minutes that we have before we run out of resources, then we can deal with Mr. Kurek's amendment and the main motion.

Instructing the chair to just send invitations to everyone on the witness list does not, I think, require a motion. It can be done on consensus.

An hon. member: Agreed.

The Chair: We were going to get to that point anyway.

The problem we have right now is that we have an amendment we need to dispose of or deal with.

If it's the consensus of the committee for us to send—

Ms. Iqra Khalid: No, sir.

The Chair: It's not. Okay, there goes that idea.

Mr. Michael Barrett: Okay.

The Chair: We're still on the amendment, Mr. Barrett.

Go ahead.

Mr. Michael Barrett: Chair, that we dedicate as many meetings as possible to complete the witness testimony.... "As many meetings as possible" is, I guess, limited only by the resources of the House. It's not as many meetings as necessary.

I don't think having meetings for the sake of having meetings is going to accomplish what we need to do. Also, making sure that we actually have business to populate "as many meetings as possible" would be important.

If we're sending a summons to folks who have already declined.... We found ourselves in this situation at this committee before, which netted the same result with folks not headquartered in Canada. We saw that with the CEO from Meta before. I would expect that should the CEO of TikTok, the parent company, not be in Canada, we would receive a similar response.

Not having limitless meetings is important. We have meetings that are programmed already, and we have....

I'm sorry, Chair—

A voice: [*Inaudible—Editor*]

The Chair: Actually, we can't go to a vote. He still has the floor.

Mr. Michael Barrett: I can't hear what they're saying.

The Chair: Go ahead, Mr. Barrett, please.

Mr. Michael Barrett: I think that having unlimited meetings when we can't even get witnesses to fill the meetings we already have scheduled is not a prudent use of the committee's time.

You've just seen that there isn't even the will of the committee to act on the proposed amended motion or the unamended motion, and that's just to send invites to all the witnesses. To just remove item (a) by having the committee agree to it on consent or unanimously agree to it.... The mover doesn't even agree to item (a) in the motion. I'm not sure how we're going to find concurrence to get through that.

Certainly, with respect to item (c), I think it's going to be important that we get a vote on that because "as many meetings as possible" is not a reasonable turn of phrase. It's not a reasonable instruction to the committee.

● (1745)

The Chair: We're still on the amendment to remove paragraph (c).

We have a hard stop right now. I'm going to have to adjourn the meeting, because it's just been indicated....

Mr. Damien Kurek: I'll pass.

The Chair: I'll give you a quick second here.

Go ahead.

Ms. Iqra Khalid: Mr. Chair, I would really implore you to get the votes in for the amendment. Let's vote on this motion as quickly as possible.

Mr. Michael Barrett: Do we have time or not?

Ms. Iqra Khalid: Again, this is further delaying the study, Chair.

The Chair: That's the difficulty. If there is more debate on the amendment or on the motion.... I can't force a vote, Ms. Khalid. I just can't.

On the amendment, is there any further discussion?

Mr. Michael Barrett: Do we still have resources to continue the meeting?

The Chair: We don't right now. We're done at 5:45.

Ms. Iqra Khalid: Chair, would it be possible to ask for resources?

The Chair: I'll leave that to the clerk to respond to.

We've been emailing some of the technical people, and we've been told that we have a hard stop at 5:45. We're past that point right now.

Mr. Michael Barrett: We should adjourn.

Ms. Iqra Khalid: I'm not sure, Mr. Chair, if there's anybody else on the speaking list.

The Chair: Mr. Kurek is on the speaking list.

Go ahead, Damien.

Mr. Damien Kurek: Thanks, Chair.

In regard to my amendment, I think it's pretty straightforward and it will be the evidence required to find out whether this motion is in good faith or is simply an attempt to hide from accountability. With that, I would simply leave those comments.

I think that part (c) of Ms. Khalid's motion is not only unprecedented but also a clear attempt to not allow this committee to look at other important matters that are at hand.

With that, I would cede my time to whoever is next on the list when it comes to the amendment.

The Chair: I don't have anybody else on the list.

Ms. Iqra Khalid: You can call the question on the amendment.

The Chair: I'll call the question.

Mr. Michael Barrett: Can we get a recorded vote, please?

The Chair: We'll have a recorded vote on the amendment.

We're going to have to do this real quick, Madam Clerk. Go ahead.

(Amendment negatived: nays 7; yeas 3 [*See Minutes of Proceedings*])

The Chair: The amendment was defeated.

I can't do this. I can't take any more.... We have competing committees here tonight. We have finance and OGGO that are dealing with this. The clerk has advised me that I can't....

We're on the main motion. I can't do this, so I'm going to have to—

Mr. Damien Kurek: Will you maintain the speaking list for next time?

The Chair: The clerk has just advised me that if there's a desire to continue this, I just need to confirm the speaking list for when we resume this and whether there's a desire to resume this on December 4. We have witnesses on the 29th.

Is there a desire to have a speaking list when we resume? I see several hands.

I'm going to adjourn the meeting.

An hon. member: Yes.

● (1750)

Ms. Iqra Khalid: Mr. Chair, if it's okay, I mean, if it's just a quick vote on the main motion, can we—

Mr. Michael Barrett: Are we adjourning or not?

The Chair: We're adjourning. Look, I have speakers on the main motion.

Ms. Iqra Khalid: I apologize.

The Chair: I can't continue this, so I'm going to adjourn the meeting.