HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

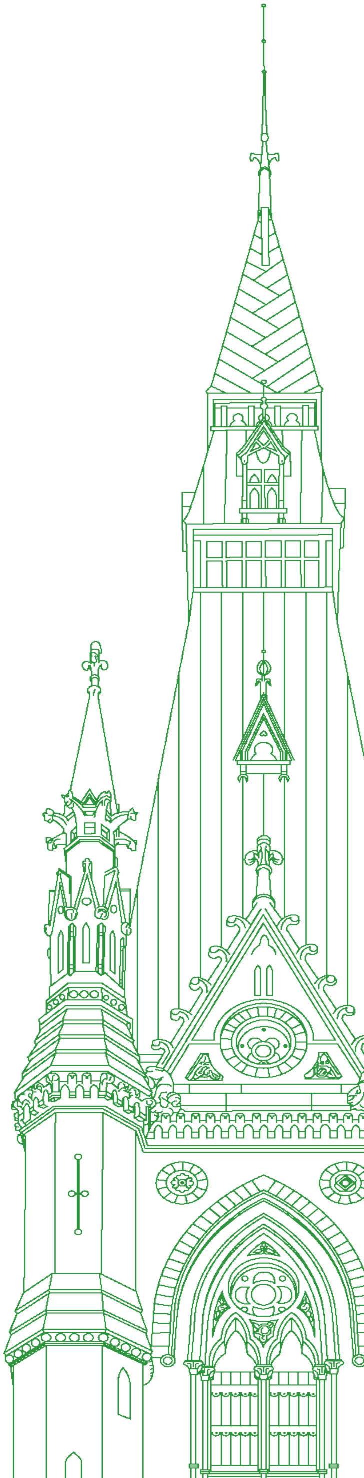
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 115

Thursday, May 2, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Thursday, May 2, 2024

● (1230)

[*English*]

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

Welcome to meeting number 115 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

Pursuant to Standing Order 108(3)(h), the committee is resuming its study of the impact of disinformation and misinformation on the work of parliamentarians.

I want to remind everybody to be mindful of their microphones. I'm not going to go through the list of things that I have to say, but when you're not using the earpieces, make sure they're in the proper place.

For those online, for the benefit of the interpreters, try not to talk over each other. We want to avoid any injury during these hybrid sittings.

I'd like to welcome our witnesses today. We are only going to have one hour; we are in the process of rescheduling the second panel to a later date. Unfortunately, with all the votes today, we're in this position. I apologize to those witnesses.

I'd like to welcome, for the first hour, Mr. Ben Nimmo, who's a threat investigator for OpenAI.

I've also got Mr. Joel Finkelstein, who is the founder and chief science officer from the Network Contagion Research Institute.

Mr. Sanjay Khanna was supposed to be on our second hour. He was here in person in the audience, so I have taken the liberty of asking him to join us for this panel. He is here as an individual and is a strategic adviser and foresight expert.

Mr. Khanna, thank you for accommodating us.

I'm going to start with you, Mr. Nimmo. I understand that you've only got until one o'clock. Again, I apologize for the votes.

You have up to five minutes to address the committee. My job is to keep things on time, so I will stop you right at five minutes.

Mr. Ben Nimmo (Threat Investigator, OpenAI, As an Individual): Thank you, Mr. Chair.

Thank you all for being here.

I would like to point out that I am speaking today in my personal capacity as somebody who has been studying covert influence operations for a long time. I've been doing this job for a decade, and it's particularly welcome to be in a conversation like this here, because 10 years ago conversations like this were not happening. There was not a general awareness of covert influence operations in the larger world of disinformation. The fact that we now have such a thriving defender community and such a thriving conversation is an enormous step forward, and that is something to welcome.

Whenever there is a large conversation like this, it is very important to have clarity over what we are focusing on, what we are talking about and how we measure what we're looking at. There are a couple of points I will make. I will try to keep it very brief.

First of all, when we talk about covert influence operations, which has been my specialization for a long time, a lot of the conversation tends to be around the content they post, because that's the thing that is most visible, and often it's the most easily identifiable. But there's a very useful framework, created by a French scholar called Camille François, which is the ABC framework. It divides influence operations into actor, behaviour and content. When you think about the ways in which the defender community can intervene, the way we can expose and disrupt this kind of operation, it's the middle portion—the behaviour—that is actually the most essential to focus on. In the space of influence operations, if you look historically, most of the content they have posted over time has not actually been the kind of content that would violate any terms of service. It would be the expression of opinion—I support this politician or I do not support this politician.

What was troublesome about this kind of operation was the use of fake accounts, the use of coordination and the use of perhaps fake websites they were building on and fake distribution networks. My work has been very much focused on the behaviours that threat actors go through. When we think about the responses the defender community can come out with, it helps to look at these operations as a series of steps they go through, a series of behavioural procedures, which might begin, for example, with registering an email address, registering a web domain or setting up social media accounts. Then for each of those steps, we have to start thinking about appropriate responses to that step and the appropriate person to do those things.

Last year, with a former colleague, I published a paper called “The Online Operations Kill Chain”, which describes how you can actually sequence and set out the behavioural steps that operations like this can go through. I've shared that with the committee, so I hope you all have access to that already.

That's about the behaviour these operations show. It's also worth thinking about the actors that are behind these kinds of covert influence operations, because sometimes there's a state actor, and sometimes there may be a commercial actor. You do find companies out there that offer influence operations for hire. Then the question becomes what the appropriate response is to a different type of actor in the space. But whenever we're talking about covert influence operations, it's also really important to ask whether they are having any impact and whether we can actually observe that a specific operation is having a specific impact. Historically, a small number of operations have visibly had an impact—most notably the Russian hack and leak operations in 2016 targeting the U.S—but in my experience as an investigator, far more of the operations that have been exposed have not managed to reach real people. They've posted stuff on the Internet, and it has stayed there. There was a Russian operation called “secondary infektion”, for example, which between 2014 and 2019 posted hundreds of pieces of content across hundreds of different platforms, none of which appears to have been seen by any real people. So influence operations are not all equal. We shouldn't treat them as such, and it's important to ask whether there is a way we can measure how far they are actually reaching.

In 2020 I wrote a paper called “The Breakout Scale” on how to assess the impact of various different influence operations and see whether they're actually going somewhere or not. This is a really important thing to be thinking through, because one of the things that operations try to do is to make themselves look powerful even when they're not. They will try to generate fear, even when there's no reason to have that fear. For example, before the U.S. mid-terms in 2018, the Russian Internet Research Agency claimed to have already interfered in the election, whereas in fact, what had been happening was that they'd run maybe 100 Instagram accounts, which had already been taken down. Having a tool that allows us to measure the impact or even to estimate the impact of these operations is critical to the conversation.

● (1235)

Again, that has been shared with the committee.

When we think about—

The Chair: I'm sorry, Mr. Nimmo. It's been five minutes. It goes quickly.

As I said at the onset, you're on limited time here. I would encourage you to submit to the committee any other thoughts that you may have—either comments or responses—after you hear some of the questions today.

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

Mr. Joel Finkelstein (Founder and Chief Science Officer, Network Contagion Research Institute): Thank you so much.

I'm Joel Finkelstein, the chief science officer and the founder of the Network Contagion Research Institute.

Our organization profiles a lot of different threats that are facing governments, democracy and vulnerable communities. There are two that I want to bring to the attention of lawmakers today because I think they're highly emblematic of the kinds of threats that lawmakers often can't see, that platforms themselves have challenges policing and that have the capacity—I think intrinsically—for a profound breakout in the near future in ways that I think could create terrible harms for society and for vulnerable communities.

The first one that we talk about a lot is child harms. There's been a surge of online child harms through deceptive practices using AI.

The second is platform-scale manipulation by state actors. In this case, we're talking about TikTok.

In the first case, we found that there were cyber criminal syndicates in west Africa using AI to impersonate beautiful women—complete with videos, pictures and images. They would speak to teenagers. There was a 1,000% increase of these cases where they would impersonate women to get these teenagers into compromising positions and then “sextort” them. This has created a rash of 21 suicides—with several in Canada—of troubled children who have been sextorted this way.

You can well imagine the application that this is going to have towards the elderly. Platforms are terrible at policing this. This criminal syndicate from Nigeria was passing out manuals on how to do this on TikTok, YouTube and Scribd. This is facilitating a breakout of this kind of crime, which is only one example of something that has the capacity to be severely disarming to lawmakers as it begins interfering with other processes, among the elderly and youth.

These kinds of catfishing schemes and harms are very challenging to police. We need investigative mechanisms to understand them and unearth them more rapidly in order to address them. I sent you reports on that and I encourage everyone to take a look.

The other issue is not just that you have individual actors who are empowered by technology, but manipulations of entire platforms. NCRI performed research on TikTok, with its 1.5 billion users, and looked at inexplicable discrepancies in material that was sensitive to the Chinese Communist Party. This looked at whether the hashtags were on Israel, Ukraine or Kashmir or whether they pertained to Tibet or the South China Sea.

We saw in some cases it was 50 to one that these were more prevalent on comparable platforms than they were on TikTok, which suggested to us an incredible discrepancy that argued for a mass suppression of information and promotion of others through a charm offensive.

Genocide denial.... These problems are rampant on TikTok in a way that creates an “Alice in Wonderland” reality for 1.5 billion users. Our social psychology analysis suggests that this is impactful and alters the psychology of users towards a more friendly, pro-China stance on a massive scale.

Understanding these kinds of problems requires that parliamentarians and democratic bodies have greater insight and investigative capacity rapidly at their fingertips to be able to explore and understand emerging threats before those threats can get the better of them.

I will cede the rest of my time.

● (1240)

The Chair: I kind of wish you wouldn't, Mr. Finkelstein. You had me glued there. I'm sure members of the committee will have lots of questions for you.

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

Mr. Sanjay Khanna (Strategic Advisor and Foresight Expert, As an Individual): My respect for your work as legislators and parliamentarians is implicit in my remarks.

As a strategic foresight consultant, I advise business, government, higher education, NGOs and registered charities about comprehensively and strategically thinking about the future. Once clients understand plausible scenarios that they may face, they can prepare for disruptions. I propose to this committee that parliamentarians must thoroughly prepare for uncertain futures.

Today Canada is less resilient than it was prepandemic. Many of us feel highly distressed, experience a more challenging economy, view politicians and institutions with greater distrust, and face the toxic consequences of polarization online and in real life.

We are living through multiple converging and overlapping crises, geopolitical instability, climate impacts, emerging diseases and technologies that fuel misinformation and disinformation. The RCMP's heavily redacted report indicated similar foreboding threats in Canada's near future. At this crossroad, I believe that Canada faces two stark choices: to build resilience to reveal falsehoods and ascertain truth with coordinated and holistic efforts or to see resilience neutralized through individualized and fragmented responses.

I harbour grave concerns about what governing might be like in a future where parliamentarians and Canadians are unable to differentiate facts from mis- and disinformation and ultimately act contrary to their individual, community and collective interests.

Parliamentarians' work influences all persons living in Canada. While all of us, including your constituents, are targets of mis- and disinformation, you as parliamentarians are at increased risk of being targeted because of your time-honoured political and legislative roles. Multiple anti-democratic actors, nation-states, criminal entities and advocacy interests seek to subvert or co-opt parliamentarians by amplifying mis- and disinformation from individual to population scales.

Canada's adversaries seek to obstruct parliamentarians' deliberative decision-making and stakeholder engagement. This threatens Canada's domestic and foreign policy, thereby challenging Canadians' economic prosperity and social cohesion. It is a common misconception that these efforts are easily detected, but subtle manipulation of a single piece of information can be easy to miss. Targeting of your trusted staff, departments and the agencies you rely on for research and analysis creates new information vulnerabilities.

Mis- and disinformation exploit technologies of social media, machine learning and artificial intelligence that parliamentarians increasingly depend on for democratic engagement and constructive action and that our economy depends on for competitive advantage. By design, mis- and disinformation are threat multipliers. They promote distrust of bedrock institutions such as the Parliament of Canada, the justice system, fact-checked media, non-partisan research, universities, health care providers and the international institutions that arose after World War II to foster co-operation and stability.

Politics of rage and grievance driven by mis- and disinformation instigate polarization at individual, group and population levels. In this environment, parliamentarians must determine if and how their positions on policy, funding and legislation may unwittingly serve Canada's adversaries or be influenced by any entity that could compromise Canada's resilience.

Parliament needs to be seen to balance mis- and disinformation with the broader contextual perspective expected of trusted institutions behaving in the national interest. Establishing cohesive whole-of-Parliament and whole-of-society approaches to addressing this mis- and disinformation is a critical mission to rebuild trust and social licence.

Parliamentarians need no reminder that Canada's enemies are pleased for us to be divided, rendering Parliament incapable of acting in the national interest, protecting agri-food supply chains, building climate security, strengthening energy and transportation networks, and securing our elections. For parliamentarians, ensuring that mis- and disinformation do not interfere with cross-party collaboration in the House is necessary for Canada's material wellbeing and physical and mental health.

Parliamentarians and their staff need to continuously learn about how sophisticated approaches to deception and/or impersonation of legislators via convincing AI-driven manipulations of video, voice, text and images may irreparably harm political reputations and our democracy.

In the short term, as Canada navigates an era of multiple converging crises, the structured approach of scenario planning can assist parliamentarians as they devise resilient public policy, legislation, regulation and stakeholder engagement. In the longer term, consider the potential for a Canadian charter of digital rights and freedoms to articulate responsibilities and protections for Canadians related to mis- and disinformation.

● (1245)

Thank you.

The Chair: Thank you, Mr. Khanna.

We're going to start with our first six-minute round. I want to advise the committee that, if we need a little extra time before question period because some of your questions are not being answered.... It's not whether they're being answered but whether you have more questions you would like to add. We can extend for another 15 minutes if we need to. As we get closer to the bottom of the hour, I'll see whether there's a desire to move on.

Okay, Mr. Barrett, we're going to start with you for six minutes. Go ahead, sir.

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

At the top of my time, I'm going to give verbal notice of a motion. I'm not moving the motion, but I'm going to give notice of it. That will give the opportunity for it to be received by the clerk, translated and distributed to members of the committee. Of course, the provision of 48 hours would then be in effect before it could be moved.

The Chair: Okay, go ahead on the verbal notice. I'm not stopping your time, Mr. Barrett.

Mr. Michael Barrett: This week, Chair, Global News revealed two investigative pieces they've been working on.

The first is one I mentioned yesterday. It's on a series of meetings between lobbyist Kirsten Poon and high-level political staff across multiple federal departments. Those meetings aimed at securing $110 million in federal grants for the Edmonton International Airport. These efforts occurred between 2021 and 2022 and involved Poon's connection to Justin Trudeau's cabinet minister Randy Boissonnault, who represents Edmonton Centre. Mr. Boissonnault, in transitioning from his consulting business to his ministerial role, delegated control of his business to Poon, who resumed his lobbying activities.

Now, Mr. Boissonnault gave his former business partner his only client, which was the Edmonton Regional Airports Authority. The minister's influence, of course, is attached to that transfer. This firm lobbied the Edmonton airport authority, an organization regulated by the government on federal government land with board members appointed by the government—the same government Mr. Boissonnault is now a member of. Mr. Boissonnault was collecting payments from the company that was lobbying his government. This, of course, raises incredible concerns with respect to the Lobbying Act, the Conflict of Interest Act and the Conflict of Interest Code for members.

Now there's a second report from Global News revealing that Justin Trudeau's cabinet minister Randy Boissonnault remained listed as a director of the Global Health Imports Corporation, or GHI, for over a year after his 2021 election. Mr. Boissonnault claims that he's had no involvement with GHI since his election, but the company co-founded by Mr. Boissonnault in 2019 after his electoral defeat secured contracts totalling $8.2 million from other levels of government—provincial and municipal—for pandemic supplies.

Now imagine the disadvantage when competing for government contracts against a company that has a member of Justin Trudeau's federal cabinet listed as one of the directors. That's why such a scenario is in fact prohibited by law. I would be remiss not to mention that GHI faced multiple lawsuits for unpaid bills and unfulfilled deliveries, resulting in default judgments totalling over $7.8 million. Allegations of wire fraud were made against Mr. Boissonnault's GHI co-founder Stephen Anderson in one of the lawsuits. Despite winning lawsuits, suppliers struggled to recoup owed funds from Minister Boissonnault's company, which he was still listed as a director for, raising questions about the legitimacy of its operation and the fairness of its bidding process.

Chair, the motion is that:

> Pursuant to Standing Order 108(3)(h) and in light of new media reports, that the committee undertake an immediate study into Minister Randy Boissonnault and allegations of fraud and contravention of ethics and lobbying laws; that the committee invite Minister Randy Boissonnault, Kirsten Poon, Stephen Anderson of Global Health Imports and the Ethics Commissioner to testify individually, in addition to any other relevant witnesses; and that the committee report its findings to the House.

Chair, I'd like to share the rest of my time with Mr. Viersen.

● (1250)

The Chair: The motion is on notice.

Go ahead, Mr. Viersen.

Mr. Arnold Viersen (Peace River—Westlock, CPC): Thank you, Mr. Chair, and thank you to the witnesses for being here today, particularly Mr. Nimmo.

I'd like to start with you around misinformation and disinformation.

I like your “influence operations” deal. One of the challenges that I have seen is around what goes and what doesn't go. It's not necessarily that it's wrong information; it's just that some things are promoted aggressively, and other things that you would think would become viral don't become viral. I'm just wondering if you have any take on how actors can manipulate things to push things that go forward and repress things that should probably go forward.

The Chair: You have 45 seconds, Mr. Nimmo.

Mr. Ben Nimmo: Thank you.

I'd actually pick up on a point that Mr. Khanna made. Something we have regularly seen, and something I have seen in many different roles, is that influence operations will try and land their content in front of a particular influencer, celebrity or politician in the hope that they will then amplify it themselves. To Mr. Khanna's point, there is a real need for great caution by all of us. Every one of you in the room is a celebrity in your own way. There's a need for great caution because quite often threat actors will not try and land something directly in front of a viral audience; they will try and land it in front of some kind of springboard, and anyone who has a social media following is that potential springboard. That can be the way in which things break out, hence the need for a kind of legislated resilience and care.

The Chair: Thank you, Mr. Nimmo and Mr. Viersen.

Mr. Housefather, you have six minutes. Go ahead, please, sir.

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

Mr. Nimmo, I have just a short question. Do you know whether Meta uses its algorithms to amplify hateful posts in order to monetize the platform?

Mr. Ben Nimmo: Mr. Housefather, I'm not sure if the committee members are aware, but I no longer work at Meta. I have not worked there for a couple of months. When I was working there, I was a threat investigator specializing in influence operations. I do not know about the ins and outs of the algorithmic methods there.

Mr. Anthony Housefather: Fair enough. I wasn't sure if your non-disclosure would prevent you from answering that either, but I was just wondering because we've had Meta witnesses before and they haven't exactly been forthcoming.

Mr. Finkelstein, I'm going to turn to you. I'm familiar with a lot of the work that you've done, and some of your most impressive work relates to anti-Semitism—how anti-Semitic tropes are spread on social media and how misinformation is fed from social media and then amplified to the extent that it comes out in the real world.

Can you give us some examples of that?

Mr. Joel Finkelstein: I wouldn't even know where to start. I think that the problem has become so prolific.

I think that there are historical reasons; that's true. The hatred of Jews is a fairly high-octane hate. It's very powerful. It has a 1,000-year history, or a 3,000-year history or whatever, to draw upon in order to inform critics and people who are looking for something to blame.

One of the things that we discussed earlier is that in the current information environment, it's so complex that the people who win are the ones who are most successful at playing the blame game. When that happens, the groups that have historically been best at receiving that blame end up being highlighted.

It's really not different from other forms of hate; it's just far more elaborate, robust and systemic. I think a lot of what we're seeing now is unusual, and there's an anomalous rise in anti-Semitism. This has been drafted deliberately. There have been efforts going back to the Soviet Union and to others to agitate for a blood libel in the United Nations and other places to accuse Israel of genocide and to say that what's happening in Israel amounts to grotesque violations of human rights that don't occur elsewhere and are unique to the Jewish people and to Israel—to one and only one nation.

The way that has been amplified across college campuses in the face of recent aggressions in Israel has led to spill-out where we definitely know that these signals start online, and they forward-predict anti-Semitism.

It's not just that the systems exist in and of themselves. We know that where we see the strengthening of these blood libels and this high-velocity political language is where the geographic signature of that language will predict where anti-Semitic attacks take place. The temporal signature of that information will predict when they take place and not the other way around.

We know that the social media signal is carrying something that is potentially instructive. That's what's important to understand about this dynamic. It's highly manufactured by enemy nations. It's perfect for creating blame and uncertainty in already-fraught societies. The result is we see that being pushed on very deliberatively by the CCP and very deliberatively by enemies of democracy because they know it's going to be successful.

● (1255)

Mr. Anthony Housefather: Would you say that Russia, for example, and Iran are behind disinformation on social media—on platforms like TikTok, YouTube and Meta—in order to convince people to accept anti-Semitic tropes and disproportionate blame on Israel?

Mr. Joel Finkelstein: Very famously, the Soviet information.... It wasn't called the GRU at the time, but it had a swastika campaign in the seventies in Europe. It decided it would paint swastikas everywhere. This goes to Ben's point about successful versus unsuccessful disinformation operations and what characterizes signal and what characterizes noise. Oftentimes, what becomes signal is concerned about noise, right? What happened in Europe was that 70 swastikas were put up by GRU members. That's all it took. That's all it took for people to start becoming convinced that everybody else was hateful. Once they were convinced that everybody else was hateful, they started blooming up organically.

So, you have a catalytic process whereby people are oftentimes initially.... You know, what's happened in social media is the growth of what we call false polarization. We're told that the other side has become so radical. Don't believe it. It's not true. Consistently, when we poll people to understand what their positions are, what we learn is that we have far more consensus on virtually any issue than what is depicted on social media, so we're being fed a conflict. In that environment, the suspicion of being undermined by a fifth column or the suspicion of having your control taken out from under you, being sold on that conflict, is where it becomes so important to say, “Hey, guys, this is a small signal. It's not that important.” However, when there's no one trusted to be able to say that, all the suspicions have fuel to become fire very quickly.

Mr. Anthony Housefather: Based on all the data that you are talking about, that these investigations that you and others are doing are providing, how do parliamentarians reliably obtain this type of data? How do we close the gap between what you know and what we know?

Mr. Joel Finkelstein: You know, I said in the podcast we were talking about earlier that I really feel that what's needed for democracies is a rapid investigatory function to be able to help really visualize the difference. Let's imagine. Let's go back to Europe. Let's do the experiment. Seventy GRU people are putting up swastikas. Instead of saying that everyone is doing it, the headline is that this is 70 people and that we're not as bad as we suspect each other of being. That becomes the headline. We aren't bad people, right? We're being presented with complexity that we've never had to deal with before, and that explains a lot of our bad behaviours and bad choices.

● (1300)

The Chair: Thank you.

Mr. Joel Finkelstein: Ultimately, when people are aligned, it's possible—definitely possible—for us to have sensible, common-sense and consensus-driven conversations that are productive, as long as we have the capacity to separate out signal from noise.

The Chair: Thank you, Mr. Finkelstein.

I'm finding it difficult to cut you off. I find the information that you're providing fascinating.

Mr. Joel Finkelstein: John, would you mind talking to my wife about that?

Voices: Oh, oh!

The Chair: If you talk to mine, yes.

[*Translation*]

Before I turn the floor over to Mr. Villemure, I want to let you know that he will be asking his questions in French. I mention it for the witnesses whose preferred language is English.

[*English*]

I'm just going to give a second for Mr. Khanna to set up his earbud.

[*Translation*]

The information being shared with the committee today is very important, so I want all the witnesses to understand what we are saying.

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

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

Thank you to the witnesses for being with us today.

Mr. Finkelstein, I'll start with you.

[*English*]

You said that "we're being fed a conflict."

[*Translation*]

I'd like to look at the situation at a broader level. Oftentimes, when I talk to people in Trois-Rivières about the Ukraine-Russia war, for instance, they tell me that everything they're hearing indicates that Ukraine is good and Russia is bad. The same can be said of many other conflicts.

To some extent, we are all targets of a narrative being pushed on us by social media or, I fear, sometimes even news agencies or media organizations with a wider reach.

How are ordinary people supposed to navigate that to get a clear sense of the issue? In the example I just gave, the message is that Ukraine is in the right and Russia is in the wrong. That may well be true, but how are people who aren't experts on the issue supposed to make up their minds?

The Chair: Which witness is that for?

Mr. René Villemure: The question is for Mr. Finkelstein.

[*English*]

Mr. Joel Finkelstein: It's a great question.

My father once had great advice. He said that it's not good to put people on pedestals because eventually everyone needs to pee.

It's sound advice in this case. It's important that we understand our own faults and it's important that we understand the faults of our allies. That's part of what it means to be able to have honest conversation. Looking at uncomfortable facts and being able to deliberate them in ways that don't leave us in fear of uncertainty of.... What if people can't handle the truth?

When we can stare at the uncomfortable facts, warts and all, then we're always in a better position to manage threats more strategically. That means we need a vote of confidence to be able to talk about those things, and amplify and elevate honest and hard conversation.

It's really ironic. People are so worried about what happens if we know the truth about what's happening and maybe our allies aren't as good as we are—

[*Translation*]

Mr. René Villemure: Thank you, Mr. Finkelstein. That answers my question. Sorry to cut you off, but I have more questions to ask.

It's said that the atomic bomb is what ended the Second World War. Today the claim seems to be that artificial intelligence will be the tool of choice in the next war, with its capacity to spread disinformation.

Are we at war?

[*English*]

Mr. Joel Finkelstein: That's such a good question.

Going back to what we were saying about whether or not we trust each other, the real question is whether we trust ourselves.

The danger that AI poses, especially generative AI, is it can trigger what's called an authenticity crisis. You won't know if you're talking to a real human. You won't know if the response you got was from somebody who's deliberate or if it's the most elegant, dexterous and successful autopilot that's ever been created. You won't know the difference. You won't be able to tell who you're talking to online. You won't be able to tell whether or not there's a real person who's agreeing with you or disagreeing with you.

I think that's—

● (1305)

[*Translation*]

Mr. René Villemure: Thank you. That is definitely scary.

My next question is for Mr. Khanna.

What does the future look like as far as misinformation and disinformation go? As it is, weak signals are being amplified. Information is spreading more and more quickly, and the idea of the truth tends to get lost. People are practically willing to replace truth with likelihood, the almost truth. At the very least, people are more likely to believe what they're told than to try to figure out what's true.

What's the outlook, then, when it comes to weak and strong signals?

[*English*]

Mr. Sanjay Khanna: If we don't really think about this deliberatively, cohesively and with strategies both for Parliament and for citizens, we're going to move more deeply and more quickly into the world that Mr. Finkelstein has mentioned.

I've done work looking at the emergence of these technologies now for 20 years. We are seeing things get to the point where they are starting to cause confusion in the public. They're starting to cause confusion among youth.

We have to think about children, I think, fundamentally. Are we doing the things today that will serve children in being able to understand and trust the environments they're living in and the context they're living in?

That's the futures orientation that I think we need to have. However, we do require a structured approach to think about what these emerging scenarios are and what we can do today to protect and mitigate against those risks so that we are resilient enough to not be manipulated at individual scales as citizens or more broadly in various groups that we participate in, and to make decisions and use the resources we have to take action to both protect ourselves and find opportunities in a changing world.

[*Translation*]

Mr. René Villemure: Thank you.

Mr. Finkelstein, I'm coming back to you with a quick question. Is TikTok a tool for disinformation?

[*English*]

Mr. Joel Finkelstein: I think TikTok has profoundly different uses from other platforms. It is primarily a platform where children and young adults can put up zany videos for 15 seconds of themselves doing obscure and nutty things, but in addition to that, it obviously serves an incredibly unusual purpose in distorting reality for 1.5 billion people at a massive scale.

This appears to be deliberate, and that makes it unparalleled, because, where you can have mob mentality and you can have prevailing political interests that are somewhat recognizable on the platforms that most people inhabit, here you have something that's quite distinct. It's a different animal. The things it produces are of a higher scale, and we're seeing far different outcomes psychologically for its users. Those concerns were crucial in us speaking to Congress and also to the Senate as they passed legislation in the United States that arrived at this conclusion: that there was something anomalous about the behaviour of the platform that merited significant concern.

Now, the process for managing that is imperfect, because we still don't know how to gather and make deliberative decisions about these large-scale platforms and how they're influencing us, but the actions of parliamentarians have to be informed by sober knowledge about the threats that are growing on these platforms. That is especially the case when those threats are coming from near enemies. My sense is that—

The Chair: Mr. Finkelstein, I'm sorry.

[*Translation*]

Mr. Villemure's time is up.

[*English*]

I didn't want that to go unanswered, because I thought it was an important part of the discussion today.

Mr. Green, you have six minutes and a bit.

Go ahead, sir.

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

I want to note and go on the record to say that my round and that of the previous speaker were limited given that we weren't able to meet the time requirements of Mr. Nimmo. I'd request that my questions be put to him in writing for response.

What I would like to do, sir, for the good and welfare of the committee, is to split the time between both witnesses present, beginning with Mr. Khanna, on high-level recommendations that he could provide within three minutes to this committee for the good and welfare of our report.

Mr. Sanjay Khanna: I would agree with Mr. Finkelstein on the question of having an investigatory capacity. I think that's important.

More broadly, I think it's really about looking at the offices of Parliament and thinking about how to protect your ability as parliamentarians to ensure what you're working with as your ground truth is based on fact: how to do that, how to train your staff and how to build their capacity to be resilient so that everyone who then interacts with you, whether it's your constituents or others, knows that you're at least a trusted source. I'm not talking about your policy positions. I'm talking about the ground truth that you're using to make decisions. I think parliamentary staff are going to be more targeted by these technologies, such as deepfake videos, manipulated voices and those sorts of things.

The other piece, then, is how you are going to protect the body of Canadian society that is your constituents and how you are going to protect the next generations. This is why I was suggesting a Canadian charter of digital rights and freedoms that outlines both the responsibilities and protections of Canadian citizens. I know that there's been a lot on the online harms act, but I don't think it clarifies to citizens what their responsibilities are and what protections may be available to them.

I'll stop there because I know we have limited time, but thank you very much for that question.

● (1310)

Mr. Matthew Green: If, with reflection and more time, you do have more, I encourage you to submit it. We can only draft our study report based on recommendations from the testimony of expert witnesses such as you.

It looks like I'm at two minutes and roughly 30 seconds, Mr. Finkelstein. You have three minutes to provide a synopsis, if you could, on high-level recommendations that you would put to this committee for our consideration at our report writing stage.

Mr. Joel Finkelstein: Thank you so much for that.

We are not a policy organization and we have refrained in our work...we have focused specifically on having a neutral attitude toward policy so that we can have a more sober capacity for risk assessment. We usually leave the policies in the hands of the experts—that's you all.

I have said this before, but I think it bears repeating. I spoke to a four-star marine general here in the United States, who commanded NATO's forces. His name is General John Allen. I asked him, “General, have you ever won a battle without a map of the battlefield?” He said it has never happened. That's what's happening with the current attempts to control social media. We have no idea what to control. We can't determine signal from noise.

Parliamentarians like you are being deliberately misled by the platforms you're supposed to be managing. As the threats emerge in the platforms, the incentives for the platforms to manage those threats are limited. They're limited because managing threats isn't their business model. They're limited by their shareholders, so I don't blame them. It's not totally their fault. Okay, I blame them a bit, but I will say that, really, the conversations we need to have need to be informed by data, and Parliament has the right to demand that data. It has the right to be able to see how the things.... Its job is to manage. It needs to be able to see those things.

I think the most important part of how we manage the threats of the future relies on a capacity for rapid research. That is the function I would most recommend that Parliament adopt—

Mr. Matthew Green: I feel like I need to be putting the question to you in the form of an AI prompt to have you imagine yourself as a legislator. What might be some of the things that you'd do as a legislator?

You talked about the commission. There was earlier commentary around the information we use as a base level of truth. Could you hypothetically comment on what accountability might look like for those that surreptitiously use these models, algorithms and platforms for nefarious use?

Mr. Joel Finkelstein: I would say there are two cases that I brought up to the Parliament for this reason.

The first is that you have bad actors who exist in closet spaces and basements and are capable of opportunistically upending...and causing mayhem and murder on massive scales. We need complete visibility of where those actors are. We need an alert system that can bring that information to lawmakers before they even know to ask for it, and we need to create a scouting capacity to understand where these emerging threats are happening so that they can be managed before they spill out into the real world.

That means we need complete platform access. We need to have the same access that platforms have, without running the risk of privacy....

● (1315)

Mr. Matthew Green: Just for the record, with the last 20 seconds, I think you suggested it should be at arm's length from the government.

Mr. Joel Finkelstein: Yes. It's crucial.

Mr. Matthew Green: We're not talking about a Big Brother model or, potentially, authoritarian capture, but an independent commission that would have.... Is that right, just for clarity?

Mr. Joel Finkelstein: One hundred per cent. If I had to tell a democratic public that their government was responsible for managing all their information, count me out. I can imagine citizens not reacting well to that, and for good reason.

Having independence is really crucial. The reason that's true is it's just like a referee. You need someone to blame, and that person has to be willing to wear the stripes and be willing to be blamed.

Mr. Matthew Green: Thank you. I think that's the end of my time.

The Chair: Yes, it is, Mr. Green.

Thank you, Mr. Khanna and Mr. Finkelstein.

Mr. Green, at the beginning, you mentioned that Mr. Nimmo should be afforded the opportunity to answer the questions. I'm going to suggest that all members' questions be forwarded to Mr. Nimmo. I feel he got a little shortchanged today because of the votes, so I want to make sure that he has the ability to respond as well. However, in typical committee fashion, we want to make sure that we have a response within a timeline, so I'm going to suggest that we get it by next Friday.

Madam Clerk, if we can share the questions with him and expect his response by next Friday, I think that would be an appropriate timeline.

If there are any other questions that need to be submitted to the clerk, or questions that are similar to the ones being asked today, I'll ask you to do that as well.

That concludes our first round. It was a very interesting round.

Mr. Brock, you're going to start us off in the second round, with five minutes.

Go ahead sir.

Mr. Larry Brock (Brantford—Brant, CPC): Thank you, Chair.

Thank you, gentlemen, for your attendance today and your very thoughtful and productive commentaries.

Starting with you, Mr. Finkelstein, I think you get the sense right now that the way committees work here in Canada is far different from how our U.S. counterparts work there. We are limited by time. At best, we are looking at five to six minutes, and you can get maybe two or three good questions in with appropriate responses.

I've been listening very carefully. Time has run out for a number of members who asked you some questions, so I'm going to give you a bit of a runway. Are there any additional thoughts, based on previous questions put to you by my colleagues, sir, that you would like to complete?

Mr. Joel Finkelstein: I have too many of them.

Mr. Larry Brock: Perhaps you could speak about the most important question, in my opinion, the one that was put to you by Matthew Green in terms of recommendations, whether they be policy or legislative recommendations. At the conclusion of this particular study, we have a mandate to report to the House of Commons. We look to the experts in the field—you being one of those experts—to help us and to guide us in preparing that report.

Mr. Joel Finkelstein: The platform that needs to be constructed for democracies isn't some faint ideal that we ought to do. It's increasingly clear to me that the lack of this organ comprises a national security crisis. The absence of the ability to make sober determinations about how democracies are being manipulated is creating an escape velocity for those manipulations, because it's disrupting the function of democracy faster than democracy can manage that dysfunction. This is a cat-and-mouse game, so what's needed is a civic network to be instantiated rapidly.

This is not needed as an idea that has to happen at some point because it would be nice. It was needed years ago. This function was needed years ago, and the goal is to step into the hardest conversations. Now, the thing about very hard conversations is that we're so concerned about them, yet the conflict is all people tend to look at. The conflict, when it's had honestly, is the solution to the problem. The conflict is the solution.

When you've structured an investigative capacity that's manned by people who are credible as good-faith actors for trying to create the most honest representation of the conflict they can create, and they're feeding that forward so we can distinguish between what's noise and what's signal here, how bad is this? Let's talk to the people who are on the other side. Let's understand what they really think about this. That's going to be an urgent thing for law enforcement to know. It's going to be an urgent thing for understanding who is really in support of our constitutions, who's really in support of the threads and the fibres that hold together our civic bonds of trust, and who are people who are seeking to deliberately undermine them.

Understanding the difference between those kinds of narratives is absolutely crucial for the functioning of democracy, so I think having a capacity to resolve the threats that bad actors, those that are hostile to democracy, are enjoying, and being able to spotlight them, we can say—

● (1320)

Mr. Larry Brock: Thank you, sir. I'm sorry; I'm going to have to cut you off. I could listen to you for hours. This really is fascinating material.

Mr. Khanna, I'm going to give you that runway as well. I know that you deliberately cut off your recommendations to this committee when Mr. Green presented the same question to you, so you have about 45 seconds, sir.

Mr. Sanjay Khanna: I think parliamentarians need to understand what resilience means, and they have to have an understanding of what you're building resilience to.

You have to look at Canada's strategic industries and how mis- and disinformation might be used to disrupt our agri-food system and food security, our national energy policy and the resilience and networks there, and, of course, election security.

I think you have to look at what our adversaries want to do to disrupt our ability to meet our own needs as well as the needs of our export markets and those sorts of things. I think there needs to be a strategic piece here that protects the Canadian economy, and I think there's a profound economic aspect to this that also needs to be looked at.

This committee does need to understand that resiliency is not infinite. What doesn't kill you sometimes does not make you stronger. Sometimes it weakens you, and the pandemic has weakened Canada. It's weakened our health status and, in national security terms, the status of the physical and mental health and resilience of each individual is seen to be the biggest defence against mis- and disinformation. That's in that doctrine. It's been the mental health and cognitive capacity of each Canadian to figure out how to act in the face of that. Thank you.

Mr. Larry Brock: Thank you. That was helpful.

The Chair: Thank you, Mr. Brock and Mr. Khanna.

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

Mr. Parm Bains (Steveston—Richmond East, Lib.): Thank you, Mr. Chair, and thank you to our witnesses.

I did have the opportunity to learn a significant amount of information from Mr. Finkelstein and Mr. Nimmo, who's now gone, and Mr. Khanna in an earlier intervention.

I'll ask Mr. Finkelstein to expand on something he talked about in his recommendations.

I think we can all appreciate that the threat is real. Our way of life, the stability of our systems and all of those things are under threat, as Mr. Khanna talked about, in a number of different capacities, whether it's our food security, the way we operate Parliament and all of these things.

I want to talk a little bit about the alert system you talked about. We already have cybersecurity teams. Where would the alert system or the independent commission of some sort come into play? Who would they alert? Would it be the social media platform providers?

Please expand on that.

Mr. Joel Finkelstein: It's a great question.

Let me just say that I'm a neuroscientist by training. I finished my Ph.D. at Princeton and was studying animals and virtual reality to reverse-engineer how their brains work using laser beams. I was not really bred in the world of intelligence, but I found that understanding how the brain works is really helpful for understanding the intelligence process.

I now train analysts, who join the FBI or CIA, at Rutgers, where I teach advanced courses on threat analysis at the Miller Center for secure communities.

What I found in that process was that when it comes to what it is we do and how to create a kind of alert function on it, it really requires that we designate the category of threat that we're talking about in ways that give it a clear set of parameters.

Really, what we're looking at is not just cybersecurity. It's social cybersecurity. Social cybersecurity is really what we train in, and the threats that pertain to it are any threat that could possibly afflict a vulnerable community or democracy.

I can give you some examples from NCRI's research as to how wide-standing that could be. This could be computer-generated hoaxes and malicious information in the wakes of mass shootings. It could be Spanish alt-right networks glorifying crusader memes. It could be bot-driven gold rushes and inauthentic social media on crypto. All of these—

● (1325)

Mr. Parm Bains: The objective is to mobilize people. Both of the things you're talking about intersect.

Mr. Joel Finkelstein: They do, and what they show is where the social risks are accumulating in ways that the institutions can't keep up with. Wherever that's happening, there needs to be an investigatory function that acts as a support system to democracy.

Mr. Parm Bains: Maybe talk about what the framework around that would be and give some simple steps.

Mr. Joel Finkelstein: The framework would be to endow and create protections for an independent entity to be permitted to amass data, especially from social media but also other other forms of database aggregation. This would create essentially a fusion centre, and it would be able to look at social cyber risks. These are risks about invasive ideologies from hostile nations invading our universities.

Across the board, it needs the capacity that's usually resolved for intelligence agencies but in ways that allow it to be aligned psychologically and aligned clinically with democracies they are protecting, and it would need protections from those democracies in order to do its job.

That's really the process. It's to create a fusion centre capacity with individuals who are reputable within the societies in question, who are aligned with the societies in question and who show clear evidence of co-operative antagonism. It would be adversarial relationships that are bought inside, not outside, in order to be credible to the vast majority of citizens, that this is something that could credibly be representative, or as close to that as possible, for the real conflicts they experience, with all the capacities—

Mr. Parm Bains: I would like to give Mr. Khanna a bit of time to expand on this, if he has anything to add.

The Chair: You have a very brief amount of time, sir.

Mr. Sanjay Khanna: Again, I'm going to get back to what the resiliency is that we need to protect for Canada and Canadians. How are you going to support your houses of Parliament and citizens to be clearer about how they protect themselves from these sorts of risks?

Mr. Parm Bains: There's an education piece there.

Mr. Sanjay Khanna: There's an education piece, but I think there also needs to be a rights framework there.

The Chair: Thank you, sir.

Thank you, Mr. Bains.

We are going to go to two and a half minutes for Mr. Villemure and two and a half for Mr. Green.

I have a budget that has to be approved for this study. If there is interest in more questions, just signal that to me and then I'll make arrangements for time to do that.

[*Translation*]

We now go to Mr. Villemure for two and a half minutes.

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

I'm going to turn to Mr. Finkelstein once again.

Earlier, I asked you whether TikTok was a tool for disinformation, and you answered. Now I'd like to ask you another question along the same lines. Does TikTok lead to a conditioning of the mind?

[*English*]

Mr. Joel Finkelstein: This is unpublished, but the data we have on this is very convincing that that is the case. I won't get into all the details, but what we see is that there is an anomalous level of belief in authoritarian ideology that's prevalent in TikTok users that is not as present on other platforms. There's an anomalous level of anti-Semitism.

[*Translation*]

Mr. René Villemure: In a publication, one researcher hypothesized that information about questioning one's gender identity may have been the result of TikTok propaganda aimed at creating chaos.

Is that reasonable to believe?

[*English*]

Mr. Joel Finkelstein: I don't know about that subject specifically, because I haven't researched it, but whenever you see polarizing issues—and the trans issue, whatever else is true, is definitely an issue that I think speaks to many people in ways that are quite urgent—you always have the capacity for misrepresentation and bad-faith conflict. That creates a scheme to capture attention really on both sides of that issue, so you have a process that should be, I think, fairly sober, "medicalized", and serious becoming something that's very highly hyper-politicized, and that's a feature of social media writ large.

So I wouldn't be surprised to find vast anti-trans campaigns parading around these places that are speaking to different adversarial groups or even other kind of hyper-ideological gender activism, on the other side, that's affiliated with revolutionary ideology and all the rest of it.

That's an example of how what should be a sober, serious conversation that is not pleasant for the people who are involved in it, I'm sure, becomes something that primarily assumes the responsibility of a public spectacle.

● (1330)

[*Translation*]

Mr. René Villemure: Can we assume that disinformation will become a military tool?

[*English*]

Mr. Joel Finkelstein: There's no presumption needed. This is used widely by state actors to cause disruption. I assume Mr. Nimmo is no longer here, because that's his specialty.

The Chair: Well, there may be an opportunity to get him back, actually, so thank you, Mr. Finkelstein.

[*Translation*]

Thank you, Mr. Villemure.

[*English*]

I have Mr. Green for two and a half minutes, and then I am going to go to Mr. Viersen for three, Mr. Fisher for three, and if Mr. Villemure or Mr. Green would like a little extra time, then we can accommodate that.

Go ahead, Mr. Green, for two and a half minutes.

Mr. Matthew Green: I've heard you say repeatedly that there's an anomalous impact by TikTok, yet I think it's fair to say that the culture wars certainly began long before the invention of TikTok, long before the invention of social media. I think culture wars have always been a primary factor used by political operatives to create wedges, to create division and to, as you pointed out, find somebody to blame. Is that fair to say?

Mr. Joel Finkelstein: Oh, they have been one hundred per cent, starting with the printing press, absolutely.

Mr. Matthew Green: *The Century of the Self* documentary on Edward Bernays outlined the way in which propaganda is used interchangeably between corporate interests and government interests and said that state propaganda is used universally by all state actors. Is that fair to say?

Mr. Joel Finkelstein: Actually, it's even worse than that. You have all probably heard of places like 4chan and 8chan, these kinds of nasty, white supremacist communities. We did an analysis of who's influencing who, Russian propaganda or 4chan. They're getting it from the kids in their basements. They're literally picking it up from the white supremacists hanging out in their basements. They're not that creative, but those kids are. And the state seizes on that and uses it.

Mr. Matthew Green: Sure, but there are also non-state actors. Isn't that right? There are ideological movements that are religious. That is not unique to any one religion. Is that fair to say?

Mr. Joel Finkelstein: It is absolutely. Every religion has its fanatics.

Mr. Matthew Green: When dealing with these topics and when looking for solutions, would it not be responsible for us to deal with the entire structure, rather than zeroing in on one ideology or one extreme?

Mr. Joel Finkelstein: It's crucial. One thing that's come out in our research is a phenomena that I term “reciprocal radicalization”.

When we look at the events that occurred in the United States—the riots that occurred during the George Floyd protests and the January 6 events—we aren't really seeing two separate events. We're seeing one event.

What happened online was that we had competing memes or competing ideologies passing out disinformation about cops—that all cops are bastards—and that democracy was a failed experiment in imperialism. That was met with vigilante activity.

Those two forces—

Mr. Matthew Green: I would pause. I feel like you've now created a bit of a false equivalency between those. These will be ideological positions—

The Chair: Mr. Green, I'm sorry, sir, but your time is up. I'm going to give you and Mr. Villemure a little more time at the end.

Mr. Viersen, you have three minutes. Go ahead.

Mr. Arnold Viersen: I'm fascinated by this discussion.

We seem to be looking for an arbiter somewhere along the line. What would that system look like?

I remember somebody tweeted out, back in 2018 or sometime, something about Colin Kaepernick getting an endorsement from Nike, while Nike paid their workers only 20¢. Snopes then did a fact check on that and they said that was incorrect and that Nike actually pays their employees 68¢ per hour, which was still ridiculous. The point was still made, but Snopes said that it was an incorrect statement.

How do we manage that? How do we build a trusted entity?

I think Snopes lost a lot of credibility when it said that.

● (1335)

Mr. Joel Finkelstein: I think you're right.

I'll go back to something I said, but I really want to get back to speaking with MP Green because I think he raised an important point that I want to address.

Really quickly, I think that's why the importance is sometimes what the exact facts are, but oftentimes, where the disinformation is really powerful, it's not actually about the facts per se; it's really about the nature of the conflict and misrepresenting how bad the conflict really is.

When we do a good job of understanding what the conflict is and we present that, people say, “Yes, that is what the conflict is about; you're not mis-characterizing my position. This is really my position”—

Mr. Arnold Viersen: Who is the arbiter? How do you bring...?

Mr. Joel Finkelstein: Ideally, you bring the people themselves. Ideally, you're surveying people themselves to capture that and you're also looking at online behaviour. There's usually a distance or a dissociation gap between those things. That distance is where false polarization comes in. It's distrust that's usually unwarranted. It's almost always what's being sold.

Mr. Arnold Viersen: That's the trouble. Who brings those actors together? Who is the arbiter?

Mr. Joel Finkelstein: I think the body that has to deliberate this has to be made up of credible adversaries. It's people who do disagree and disagree on axes that represent popular conflicts. That has to be believable to most of the people who hold those views.

They have to be able to say that this is their guy, this is really what they believe and this is why they find this person compelling.

Mr. Arnold Viersen: How do you deal with the perceived platforming of perhaps nefarious characters?

The Chair: Give a very quick response, please.

Mr. Joel Finkelstein: We have to have a process for arriving at who meets the criteria of being somebody who both holds a fairly polar position and is also an adult in the room.

The Chair: Thank you.

Mr. Joel Finkelstein: It is not always easy to make that distinction, but if you're transparent about how you've made it, you've done the best you can in bridging gaps, so you can earn people's trust.

You have to earn that. It's not going to just be given, dictated or legislated. You have to earn it.

The Chair: Thank you, sir.

Mr. Fisher, you have three minutes.

Then we're going to have to cut it down to two minutes each, Monsieur Villemure and Mr. Green, because we have members who need to prepare for non-answer period.

Some hon. members: Oh, oh!

The Chair: Mr. Fisher, go ahead.

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

Thanks to our witnesses.

I'm really concerned about the increasing prevalence and dangers of political leaders and politicians who themselves participate and feed into the machine of online disinformation and conspiracy theories.

Mr. Finkelstein, I'll ask you two quick questions. There is a very short amount of time, but if there is any spare time, we'll go to Mr. Khanna.

How can politicians and people in the public sphere protect themselves against potential threats and violence driven by online information?

What responsibility do politicians have to ensure that they're not fanning the flames that lead to potential threats and real-world danger?

Mr. Joel Finkelstein: I would say that the way that we can shore up resilience in the face of information threats is about the creation of transparency wherever that's possible. We need lawmakers who work towards creating greater transparency in their decision-making processes with the data that they're using to make decisions and showcasing that so that how you come to this conclusion is evident for anyone who wants to see it. Getting better data and being responsible about being a steward of data so you can become better informed is important. Doing more of that is the key to earning trust in this age. People may disagree with you, but if what they find when they penetrate is that they have good reason to understand that you're making a good-faith effort, it forgives a lot.

Going back to what Mr. Green said about ideological differences, I'm not talking about the BLM movement. We found out that the violence that took place in the summer was statistically and geographically of a different set of parameters than the BLM mobilizations themselves. These were a fringe group of anti-government activists and anti-police activists who were espousing not just anti-police ideas. It's okay to not think that policing is good and needs reform, but these were people who were calling for complete revolution and the murder of officials. It's those people to whom we need to be able to say, “Hey, I agree with you that we need more social justice, and I agree with you that racism is bad, but this part of it I'm not in for”. Being able to make those distinctions is really important, because we don't want to create hostility around the basis of the belief that somebody is more polarized than they really are.

When we drill down into it, it's amazing how much we have in common. That's the hidden truth that comes out beyond the social media and the hype. It's amazing how much consensus there is.

● (1340)

Mr. Darren Fisher: Thank you, Mr. Finkelstein.

Mr. Khanna, do you want to touch on that?

Mr. Sanjay Khanna: In the end, I think to some extent this goes back to how we debate very tough issues and what example we set on resolving conflicts and setting policy agendas. The children are watching, the youth are watching, and this is also what the fuel is for dis- and misinformation, particularly from state and non-state actors that want to influence us. If they were looking at certain divisions that they can exploit within the House of Commons, they will work hard to do that, and that's what I'm most worried about.

The Chair: Thank you, sir.

[*Translation*]

Now it's over to Mr. Villemure for two minutes.

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

I have a very simple question, Mr. Finkelstein. We've talked a lot about platforms and social media, but looking beyond that, I'd like to know what role companies like Palantir play in disinformation.

[*English*]

Mr. Joel Finkelstein: You might be asking one of two things. You might be asking what role private companies have in creating more resilience against this information, or you might be asking if it is possible that companies that are expert in disinformation go out of bounds and create problems?

Which one of those questions are you asking?

[*Translation*]

Mr. René Villemure: The second one.

[*English*]

Mr. Joel Finkelstein: This is something that we have dealt with in a very high-profile way with other organizations that are in the disinformation space. Disinformation is a word I tend not to like, because I think people have different opinions of what is and isn't disinformation that are polarizing.

We have called out in very high-profile cases the affiliations between "disinformation" groups and people who have revolutionary and anti-government ideologies. On the front page of the L.A. Times, we have been on the record speaking about that problem.

My sense is that there is a challenge you have with private groups, but oftentimes those groups will lose credibility. What happens is, when you do play into an ideological game, people can tell that. You'll know that's true because you'll have one side of the party pick their disinformation expert, and you'll have the other side of the party pick their disinformation expert. Now you have competing experts who are saying, "You're the disinformation agent", or, "No, you're the disinformation agent". Again, this is part of the signal that we need to be promoting.

We just got a $4-million grant at Rutgers University to create a civic infrastructure to promote positive messages about civility online with these tools.

The Chair: Thank you.

Mr. Joel Finkelstein: How do we create forward messages that promote democratic values, not just playing "gotcha" but promoting the democratic values that people need to engage in as a solution to the problems they have?

The Chair: Thank you, sir.

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

Mr. Matthew Green: Thank you very much.

I want to shift from digital disinformation to the traditional analog disinformation and the ways in which information is perpetrated that fuel the atrocities being committed around the world.

I referenced the quoting of President Joe Biden about 40 beheaded babies. It's just this horrible, atrocious dehumanization in the pretext to the incursions into Erez and other places.

Without having to get into specificity about that, can each of you just comment briefly on the ways in which traditional analog channels for misinformation and disinformation are also part of an ecosystem that are then catapulted into the universe online and in other spaces?

Mr. Khanna, perhaps you can start, followed by Mr. Finkelstein.

Mr. Sanjay Khanna: I don't have a lot to say about that except to note that the integrated approaches are the most effective. If you see something online and then you see an analog in the real world that confirms that opinion, or it's suggested to you that things in the actual physical world based on an online campaign are reflecting your beliefs online, then that's going to be another vector and a confirmation in physical space for some potentially pretty malign opinions. What I think is interesting is how sophisticated people are about looking at that confluence.

I'll now hand it over to Dr. Finkelstein.

● (1345)

Mr. Joel Finkelstein: You know, when I teach my students about this, I call it "atrocity pornography"—there's a way in which you're seeking confirmation for pre-existing biases. Why do people do that? People did that long before social media, and the reason they do that is uncertainty. When you're faced with uncertainty, it matters a lot less what the truth is, and it matters a lot more what mob you're with. The thing about mobs is that they're very effective at creating the truth on the ground: "Who cares about what the truth is? My mob and I will tell you what the truth is."

Mr. Matthew Green: Just for the purpose of the study, can you quickly define "mob" before my time runs out?

The Chair: Your time has run out, but I'm going to allow him to define that.

Please go ahead.

Mr. Joel Finkelstein: Psychologically speaking, a mob is a mass of people who are policing moral uniformity and policing in-group loyalty and loyalty to authority at the expense of critical thinking. In order to police specific outcomes in the world, it often involves a punitive orientation towards people whom you disagree with as part of the psychological characteristic of both left-wing and right-wing authoritarianism. Those are the psychological features of mobs.

Mr. Matthew Green: Thank you. That is very helpful. I'm looking forward to the podcast.

The Chair: That concludes the panel for today.

Mr. Khanna, thank you for being here, sir. Mr. Finkelstein, thank you so much for participating today. We really appreciated the information both before and during the meeting. I'm going to dismiss our witnesses.

There is one order of business that we need to take care of, and that's the study budget. The budget for this study is in the amount of $11,500 and includes the usual witness costs, plus headsets and other things.

Do I have unanimous consent for the study budget? Thank you for that.

Thanks to the clerk, our technicians and our analysts today. This was a fascinating panel, and I want to thank you again for being here.

The other thing I will discuss is that, because we had Mr. Khanna come in, I'm going to attempt to have Mr. Nimmo come back because I think he adds a lot of value to this discussion.

Have a great weekend, everyone. We'll see you next week.

The meeting is adjourned.

Published under the authority of the Speaker of
the House of Commons

SPEAKER’S PERMISSION

Also available on the House of Commons website at the
following address: https://www.ourcommons.ca

Publié en conformité de l’autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Aussi disponible sur le site Web de la Chambre des
communes à l’adresse suivante :
https://www.noscommunes.ca