HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

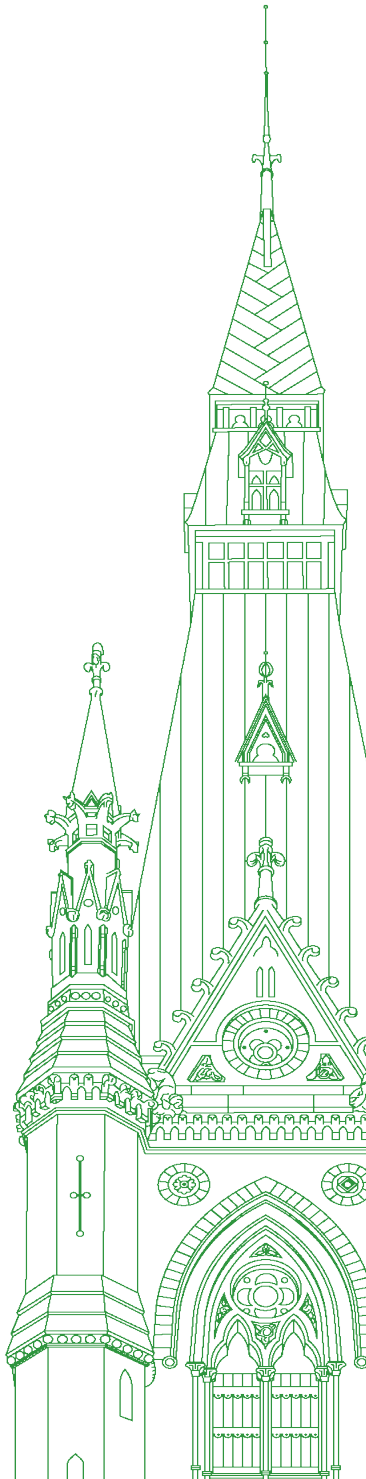
Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 092

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Monday, November 20, 2023



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Monday, November 20, 2023

● (1550)

[*English*]

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

I want to welcome everyone to meeting number 92 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[*Translation*]

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

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

[*English*]

I want to remind all members and witnesses that care must be taken with regard to the earpieces for interpretation. Please be mindful not to place your earpiece near the microphone as this could result in feedback, causing injury to our interpreters.

I would now like to welcome our witnesses for the first hour today.

From the Canadian Security Intelligence Service, we have Peter Madou, director general of intelligence assessments—welcome, Peter—and Cherie Henderson, who is the assistant director of requirements.

From the Communications Security Establishment, we have Sami Khoury, who is the head of the Canadian Centre for Cyber Security.

I am going to start with our representatives from CSIS. You have up to five minutes for your opening statement.

Cherie, go ahead, please. Thank you.

Ms. Cherie Henderson (Assistant Director, Requirements, Canadian Security Intelligence Service): Thank you.

Good afternoon, Mr. Chair and members of the committee.

My name is Cherie Henderson, and I'm an assistant deputy minister and assistant director of requirements at CSIS.

[*Translation*]

It is an honour to join you today and to have the opportunity to contribute to your important discussion on social media and foreign entities. I am joined by my colleague Peter Madou, who is Director General, Strategic Bureau.

[*English*]

Today, we hope to provide insights to this committee on the national security concerns related to data sharing with foreign entities like the People's Republic of China and the role that CSIS plays in ensuring the protection of Canada's prosperity, national security interests and the safety of Canadians.

[*Translation*]

Foreign state actors leverage all viable means to carry out their foreign interference activities, and social media platforms are ideal tools.

[*English*]

Threat actors, including the Russian Federation and the PRC, exploit media to spread disinformation, leveraging suggestive algorithms to amplify echo chambers and manipulating content for unsuspecting viewers. This utility was indeed evident in the 2016 United States presidential election, and it continues to be of concern in Canada. These same characteristics of social media are also weaponized by extremist threat actors to radicalize and recruit users.

Social media platforms are of interest to threat actors because of the data they generate and collect. Social media platforms run surveys, collate datasets and request access to users' personal data through terms and conditions, enabling access to users' photo albums, messages and contact lists. Although some of this data is benign in isolation, when collected and collated on a massive scale, it can provide detailed patterns and insights into populations, public opinion and individual networks. Canadians should therefore be aware of the privacy considerations at play when choosing to share their personal information online, especially when it is with foreign-owned companies that are based outside of Canada or our allied countries.

Authoritarian states like the PRC leverage big data, including from the private sector, to carry out their foreign interference activities. While government use of data in Canada is strictly governed to respect ethical, legal and privacy considerations, authoritarian states are not similarly limited. The PRC uses this unfettered access to harvest data at a scale that outpaces all other countries in the world combined, while fiercely protecting its own information.

Emerging technologies, such as artificial intelligence, will only further enable its nefarious activities. Through its 2017 National Intelligence Law, the PRC compels individuals, organizations and institutions—including social media platforms operating in China—to provide mass information to the Government of China. This information is then used to assist the PRC security and intelligence services in carrying out a wide variety of intelligence work. PRC-based organizations and PRC citizens are also required to protect the secrecy of all state intelligence work. This policy supports and is reflective of the PRC's bold and sustained attempts to conduct foreign interference in Canada.

It is imperative that Canada builds resilience against foreign interference. This includes bolstering awareness of the PRC's ability to harvest and use Canadians' information obtained through social media to conduct foreign interference.

For example, CSIS' X account recently posted a thread on how PRC intelligence services used LinkedIn to target Canadians by deceptively posing as interested business contacts looking for consultants in Canada, so that they would unknowingly provide privileged information that is of interest to the PRC to trained intelligence officers.

● (1555)

[*Translation*]

Now more than ever, protecting Canada's national security requires a whole-of-society effort that begins with informed and trusted discussions among communities, academia and governments at all levels. Individual users of social media need to be aware of the risks when sharing personal data with platforms. CSIS remains a committed partner in this effort, and our team of dedicated and talented professionals are working hard to keep Canadians safe, secure and prosperous.

[*English*]

I will be pleased to answer any questions.

Thank you.

The Chair: Thank you, Cherie, for your opening statement.

Next, we're going to go to Mr. Khoury, who is the head of the Canadian Centre for Cyber Security.

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

Mr. Sami Khoury (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Good afternoon, Mr. Chair and members of Parliament.

I'm pleased to be joining today's meeting. I'd like to acknowledge that we're meeting on the traditional unceded territory of the Algonquin Anishinabe nation.

My name is Sami Khoury and I'm the head of the Canadian Centre for Cyber Security, also known as the cyber centre. The cyber centre is part of the Communications Security Establishment.

[*Translation*]

As Canada's technical authority on cyber security, we use our expertise to keep safe the information and systems that Canadians rely on every day.

[*English*]

We work to protect and defend the country's valuable cyber assets, lead Canada's federal response to cybersecurity events and raise Canada's cybersecurity bar so that Canadians can live and work online safely and with confidence.

At the cyber centre, we share advice and guidance with Canadians regarding online dangers. This includes informing them how they can protect themselves and their organization most effectively from the threat social media apps could potentially pose.

[*Translation*]

We also help inform Government of Canada policy decisions regarding cyber security, including the use of social media apps, which are an important online communications tool to reach Canadians.

[*English*]

In February of this year, the Treasury Board Secretariat issued a statement announcing the ban on the use of the TikTok application on government-issued mobile devices. As recently as last week, a similar announcement was made regarding the use of WeChat. Both decisions were made by the chief information officer of Canada, who assessed that the apps in question present an unacceptable level of risk. While these bans apply solely to government-issued devices, both TBS statements led Canadians to guidance published by the cyber centre.

In our unclassified national cyber-threat assessment 2023-24 report, we assessed that foreign states are using social media to target Canadian individuals. Public reporting by the University of Toronto’s Citizen Lab detailed how cyber-threat activity has targeted activists in Canada through disinformation or intimidation on social media, denial-of-service attacks against their organizations and compromise of their personal devices.

Beyond cyber-threat activity against individuals, states are very likely using foreign-based social media and messaging applications popular with the diaspora groups in Canada and around the world to monitor communications. States can take advantage of permissive terms of use and their own legislative powers to compel data sharing. This activity threatens the privacy of the communities using these applications.

● (1600)

[*Translation*]

Canadians with commercially sensitive information on their devices should be especially cautious when granting access to their devices.

[*English*]

Not all instant-messaging apps and social media platforms are created equal. Some platforms are more responsible, where you potentially don't have to worry about the data falling into the hands of a nation-state, but other platforms are too close to that line.

The cyber centre strongly recommends that Canadians make well-informed decisions for themselves about what online services they are willing to use.

[*Translation*]

Conducting these assessments and making these decisions does not have to be difficult, and the Canadian Centre for Cyber Security has published online resources to make this process easier.

[*English*]

The cyber centre recommends researching the app or platform to determine whether it is trustworthy. This includes reading the terms of use and conditions. Find out what is being said about a particular app in the media and other trusted sources and, most importantly, know what you are consenting to. Ask yourself whether this app really needs access to your personal data, like your contacts list. While it may seem unimportant to review a platform's security and privacy functions, doing so allows you to avoid using apps that lack strong authentication protections and is well worth the time invested.

[*Translation*]

Finally, always prioritize security over convenience, and consider where your data is being stored and how this may affect your privacy.

[*English*]

In conclusion, social media has changed the way Canadians communicate, stay in touch and build new relationships.

[*Translation*]

As the social media threat landscape continues to evolve, Canadians must make sure to make responsible and informed decisions about how best to protect themselves and their information online.

[*English*]

If you can inform yourself to adopt better privacy and security protection, you could also help to support your family members and loved ones.

Again, thank you for the invitation to appear today. I welcome any questions you may have.

The Chair: Thank you, Mr. Khoury. That's great advice.

For the benefit of our witnesses, just make sure you have us on the language of your preferred choice, because you will be getting questions in both languages.

We are going to start with Mr. Barrett for six minutes.

Go ahead, Mr. Barrett, please.

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

How many illegal police stations are operating in Canada?

I'll direct the question to CSIS, please.

Ms. Cherie Henderson: I'm sorry. I had to go back a bit in my memory here.

First of all, I'm not sure that I would necessarily call them "police stations". I think what we have seen over the past few months is individuals who have links back to the PRC or who are supporting some of the work of the PRC—often, individuals who have been perhaps co-opted. At one point, we were looking at three—and it was in the media—where the RCMP was fully engaged in regard to those stations.

I wouldn't want to comment any more in regard to the activities of the RCMP.

Mr. Michael Barrett: Is it your understanding that they're continuing to operate, or have they been closed?

Ms. Pam Damoff (Oakville North—Burlington, Lib.): I have a point of order, Mr. Chair.

The Chair: Go ahead with your point of order.

Ms. Pam Damoff: Thank you.

Our study is on social media platforms. I'm trying to see the connection between our study and the questions being asked of the witnesses.

The Chair: I'm sure Mr. Barrett will make a connection at some point. I understand your point, but it's his time. I'm going to give him his time.

Go ahead, Mr. Barrett.

Mr. Michael Barrett: On the point of order, Mr. Chair, the question speaks to transnational repression. I think it's important to establish that there are foreign state actors engaged in this and what activity is done. The example I'm attempting to ask the witnesses about is perpetrated by the same state actors who are engaging in this transnational repression using social media technologies, some of which were outlined in the initial statements.

I'm not sure how much I need to qualify my line of questioning. I'm happy to go further on the committee's time, if that's what you'd like, but not in my questioning time.

● (1605)

The Chair: Thank you.

For the benefit of members of the committee, I generally try to give a lot of latitude to each member who's been given their five or six minutes, or whatever the case is. I expect Mr. Barrett is going to make a connection. He made a compelling argument there. I'm going to continue with Mr. Barrett.

I stopped your time. You have four minutes and 51 seconds. Go ahead.

Mr. Michael Barrett: Beijing conducting transnational repression activities here on our soil—evidenced by these so-called police stations, if you will—means that Chinese Canadians are being targeted for intimidation and influence. That's the purpose of these so-called police stations.

Ms. Cherie Henderson: I wouldn't specifically focus on the so-called police stations. What I would say to you is this: There is absolutely foreign interference activity happening in our country, but it can come in all forms and varieties. By focusing on just the police stations, I worry that individuals will then miss what else is happening in the environment.

Mr. Michael Barrett: I appreciate that.

Is it understood that it's a technique of the dictatorship in Beijing to scrape social media in order to isolate and target the people who are the intended targets of those repressive activities? Is social media a tool used by agents acting out of these locations to gather intelligence and then target those individuals?

Ms. Cherie Henderson: I think that's a very interesting question and one we need to discuss.

A lot of it comes down to how Canadians protect their own personal information—or any citizen of the world, let's say. If you are quite open and put a lot of your personal information out on social media, absolutely, hostile states will be able to scrape that data, regardless. It doesn't have to be China. It could be other hostile states we're dealing with. I think that's also very important. Don't lose sight of all the hostile activity directed against Canadians by focusing on just one actor. It's very important to totally protect all of your social media access and the data you put on there.

You're absolutely right in the comment you made. Hostile states will pull that information. They can collate it, crunch the big data and do very targeted attention, if they want to.

Mr. Michael Barrett: Foreign state actors don't just target the diaspora communities within our country. They also target elected officials. We've seen media reports about those efforts. In recent months, we've seen stories about a “spamouflage” campaign targeting certain politicians on their social media.

Has the dictatorship in Beijing been identified as the source of that campaign?

Ms. Cherie Henderson: Sami, would you be able to answer that particular question?

Mr. Sami Khoury: No, I can't, unfortunately.

Ms. Cherie Henderson: I'm not sure whether I could indicate that it went back to China. I'd have to go back and see what we know about it.

What I can say is that, again, you're very right. Individuals will pull all of that data and target whoever they feel is somebody they need to try to repress, want to get more information on, or want to try to influence in regard to the activities they may be engaging in.

Absolutely, social media can be used to collect the information to do that.

Mr. Michael Barrett: These are foreign interference activities. Even if you aren't able to say which foreign state actor is responsible, that's what these activities are.

Ms. Cherie Henderson: I would term that as a foreign interference activity, yes.

Mr. Michael Barrett: Are you able to say how many Canadian politicians have been targeted by foreign state actors engaging in these interference activities—just a number, if you could?

Ms. Cherie Henderson: I couldn't give you a specific number.

Again, what I would say is that every single politician, every member of Parliament, should always protect their personal information, their privacy, and be aware if somebody or an entity is trying to approach them in order to engage in some sort of foreign interference activity. It can come in all forms and shapes.

Mr. Michael Barrett: Are you able to say how the rapid response mechanism came into play in the case of the “spamouflage” targeting of elected officials?

Ms. Cherie Henderson: No, that would be GAC. Foreign Affairs is the one that manages the rapid response mechanism.

Mr. Michael Barrett: At what point is it your understanding that government is made aware of attempts by foreign state actors to target Canadians, including Canadian politicians? Is it specifically GAC, or does our national security agency, CSIS, engage at some point, obviously being aware that this is ongoing?

● (1610)

Ms. Cherie Henderson: Yes, absolutely.

Several months ago, the Minister of Public Safety issued a ministerial directive indicating that if we became aware, within the service, of negative activities directed against politicians by hostile foreign states, then we were to look at the information, determine the threat value of that information and then reach out and advise the various political actors.

The Chair: Thank you, Mr. Barrett and Ms. Henderson.

Ms. Damoff, you have six minutes.

Go ahead, please.

Ms. Pam Damoff: Thank you, Chair.

Thank you to both organizations for the work you do to keep Canadians safe. You don't get enough credit for the work you're doing behind the scenes, so I want to thank you for everything that both organizations are doing.

Specifically on TikTok, we had them appear here as a witness. They told us that the only thing they collect is an email address and the age. I'm going to ask about age in a minute. Would you say that's accurate, in terms of the information they are collecting from individuals online? My understanding is that you can gather a lot more just by what people search for, and I asked them about that. You can tell whether people have a heart condition because of what they're looking for in their searches.

I'm not sure who is better prepared to answer this. Mr. Khoury, you look like you're ready to respond.

Mr. Sami Khoury: Thank you for the question.

I think we need to distinguish a little bit between what is required to register for a TikTok account and what is being asked for to enhance user experience. There might be additional access, as I pointed out in my opening comments, to your contacts list, your calendar, or other sorts of privacy settings in your phone, in order to enhance the user experience. That's maybe the secondary offer of information that is being collected through TikTok.

Ms. Pam Damoff: They were quite adamant that no information was being shared with China and that their servers were in the United States, Indonesia and Malaysia, I think.

What led the government to ban TikTok from government devices? It wouldn't have been a decision that you took lightly.

Mr. Sami Khoury: The banning of TikTok on government devices was a decision made by the Treasury Board CIO of Canada, based on an aggregate risk level that was deemed too high. From a government perspective, the aggregation of all that information could potentially expose who our contacts are within government and our activities within government. I suspect that, from a privacy perspective, this is what led the CIO to promulgate the policy around banning the application from government systems.

Ms. Pam Damoff: I want to talk about youth, because TikTok is not alone in this.

They said that they have all of these safeguards in place so that young people are not using TikTok. I would argue that it doesn't matter whether it's TikTok or Instagram or a number of other social media platforms; youth are sharing an inordinate amount of data on their social media accounts, which can lead to exploitation.

First, I would like you to comment on youth exposure to social media platforms and whether the platforms are doing enough to limit their exposure. Also, what can we be doing, as a government, to support young people so that they know what is happening, because they don't right now?

Mr. Sami Khoury: Our concern at the cyber centre is one of raising awareness of the threats posed by social media and educating users about the privacy settings and best practices on how to use those applications—not to volunteer too much personal information and to ensure that the privacy settings on the apps are as attuned as possible to the particular user, recognizing that in some cases where the data is hosted and who has access to the data can pose an additional risk to the user. In that case, the data hosted in some countries might pose less of a risk than it would in a place like China or somewhere else.

Our role is really one of education and raising awareness about the threats posed by these applications.

● (1615)

Ms. Pam Damoff: Would you support social media platforms having their privacy terms and conditions in a more user-friendly way? You could have those things in legalese but sort of highlight what people are actually agreeing to. I would bet that 95% of Canadians don't actually read those terms and conditions when they go through them.

Do you think there should be more of an onus on them to simplify that so that you have to agree to the simplified one and the longer one?

Mr. Sami Khoury: Informing Canadians of what it is they are signing up for is absolutely important. We can describe it through our cybersecurity advice and guidance, but if it's also explained in individual apps in such a language that users understand exactly what they're consenting to sharing and with whom, that will definitely help everybody be aware of what is happening in the background.

Ms. Pam Damoff: I have only about 30 seconds left.

Are there any other recommendations that either of you would have for us that you haven't already shared, particularly with regard to young people?

Ms. Cherie Henderson: I don't have any recommendations per se, but I would like to pick up on one thing that you noted, and that was the vulnerability of our youth. What I am very worried about is that some of the youth do get onto these social media platforms and then they can get into some extremist milieu and get very influenced in a negative way. That is something we need to be quite concerned with and aware of. They make connections and they get into almost an echo chamber. That's something we need to be aware of.

The Chair: Thank you, Ms. Damoff, Ms. Henderson and Mr. Khoury.

[*Translation*]

Mr. Villemure, you have six minutes.

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

I thank all the witnesses for joining us today.

Ms. Henderson, I'd like you to provide us with more details about the links you've drawn between foreign interference, TikTok and the risks of using platforms.

Ms. Cherie Henderson: Thank you for the question. I will respond in English.

[*English*]

What I would like to explain a little bit more is the fact that a lot of individuals do go onto social media platforms and they do share a lot of information. As my colleague Sami noted, sometimes it's just what you like, and sometimes it's things that you follow. You have your camera on, or you have your pictures, and it's all up on social media. Foreign actors with a hostile intent can pull all of that information together and get a very good picture of who you are as an individual and how they might be able to influence you.

The other thing we find happening within social media is that it seems to be a very good place for trends to be noted and seen. If a foreign actor wants to determine what kind of trend might be happening in a certain area, they can keep an eye on what's happening on a social media platform: Where are people voting? What are people worried about? What are people concerned with? What misinformation or disinformation are they following? That is why I say that these are very strong tools that can actually be used to harm and to engage in foreign interference activity.

[*Translation*]

Mr. René Villemure: If I understand correctly, in order to not share that information, it's essential to read the conditions and consent to not sharing one's personal information.

Once people start using a social media platform, is it too late to step back?

[*English*]

Ms. Cherie Henderson: I don't think it's ever too late to step back, but what I would say is that in some cases the horse may already have left the barn. You do have to be a little bit worried about that, but people do change as they move forward. If you stop sharing that personal information or you are more attuned to what you're sharing, even from today moving forward, I think you will be starting to put in some protections around your social media presence.

[*Translation*]

Mr. René Villemure: You said that China isn't the only actor engaging in foreign interference. Which networks should we be very wary of, other than TikTok? Which ones should we be very careful of, and to which countries are they tied?

[*English*]

Ms. Cherie Henderson: I always hate to narrow things down, because then I worry that people will start to focus only on those threat actors.

I think everyone in this room is probably already aware that another actor we're concerned about is Russia. We are also concerned about Iran and North Korea. Those are at the top of our list at the moment, but I would say that you should think even more broadly than that and always protect whatever's on your social media account. You never know who's looking and who's trying to gather more information on you.

● (1620)

[*Translation*]

Mr. René Villemure: Thank you very much for your answer.

When we think of TikTok, we think of China. What should we associate with Russia, Iran and North Korea? Which networks could be associated with those three foreign actors?

[*English*]

Ms. Cherie Henderson: I, myself, am not fully aware of all the networks within those specific countries.

Again, as an innocent individual on a social media account, you need to try to find out where that social media account is being generating from. The more information Canadians take to get themselves informed, the more they will be protected. You may think it's not coming out of a state that we may be concerned about, but if you start to dig a little deeper, you might get there.

I would say, always double-check to make sure you know exactly what you're engaging in and whom you're engaging with, to the best of your abilities.

[*Translation*]

Mr. René Villemure: I imagine that 14-year-olds and 15-year-olds don't think to check where their data is going or what it will be used for. We know that no one reads the consent form and it's complex. No one knows where their data will end up.

How can we protect them? How can we help youth and younger people better understand what's at stake, so that they don't recklessly share their data.

[*English*]

Ms. Cherie Henderson: I think that's an extremely good question and it's an extremely difficult question to answer.

I think a lot of it goes back to what my colleague Mr. Khoury said, which is education—constant education. It's not only education for adults, but education at all levels. I'm not a policy person; I'm an operational person, but I think it would be very important to figure out ways to educate the youth and engage on that level. I think there are other government departments that can support that sort of work.

[*Translation*]

Mr. René Villemure: Mr. Khoury, I want to ask you the same question.

Mr. Sami Khoury: Thank you.

As my colleague just said, education is extremely important in keeping young people informed. In reality, it's clear that China raises somewhat more complex concerns.

Any information we put in the public domain could ultimately be a source of concern. It's important to keep both young people and not so young people informed of the risks that publishing such information could have in the future. It might not pose an immediate threat, but it can present a threat later, once a more complete portrait or profile of the individual has been compiled.

The Chair: Thank you, Mr. Khoury and Mr. Villemure.

[*English*]

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

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

I'm going to put a series of questions to you.

First of all, thank you for being here. It's always a pleasure for me, as just a working-class guy from Hamilton, to be able to ask questions of the CSE and CSIS. This is kind of cool.

I'm going to put some direct questions to you, and I'm going to ask you to answer them as directly as you possibly can.

On February 27, 2023, the Government of Canada announced it was banning the use of TikTok applications on government mobile devices. Was the Communications Security Establishment consulted when this decision was made?

This is for you, Mr. Khoury.

Mr. Sami Khoury: Yes.

Mr. Matthew Green: Was CSIS consulted when this decision was made?

Ms. Cherie Henderson: I don't know.

Mr. Matthew Green: That's fair enough.

In the consultations that you had, what feedback did you provide the government on singling out TikTok for this type of ban?

Mr. Sami Khoury: We are not a regulator and we don't assess every app out there. Our advice is how to consider the risk, from a privacy perspective, of the permissive settings that the app is requesting.

Along with the ban of TikTok, we also put out some advice and guidance on social media applications for Canadians and for Canadian businesses in general.

Mr. Matthew Green: Specific to the government and the ban, it appears to me that you have a strong rationale. You talked about an acceptable level of risk, yet all the focus seems to be on the fact that this is a state-owned actor through ByteDance.

I want to put a question to you in relation to surveillance and data capitalism or algorithmic capitalism. In other words, what's to stop Facebook, X or Twitter, or any other platform from simply collecting the same data and selling it through a third party to the same hostile actors you've identified?

● (1625)

Mr. Sami Khoury: On TikTok, just in case it didn't come out clearly, it presents an unacceptable level of risk. That's why the application was banned.

Mr. Matthew Green: What's acceptable?

Mr. Sami Khoury: Many apps that we have on our government phones are apps for which the level of risk is acceptable. In our advice and guidance on what we put on our government phones, we look at a number of things, like security control and who is behind the app.

Mr. Matthew Green: In your time with the CSE.... How long have you been with them?

Mr. Sami Khoury: It's been 32 years.

Mr. Matthew Green: You were there in 2016, and you were there in 2019, particularly, when the joint investigation by the Privacy Commissioner brought to light the Cambridge Analytica scandal in Facebook.

Mr. Sami Khoury: I was at CSE. I wasn't in my current role, but I was at CSE.

Mr. Matthew Green: Were you advising on that as well? Did you have any knowledge of that as well?

Mr. Sami Khoury: I wasn't in a position where that was my task.

Mr. Matthew Green: You would recall that this British consulting firm, Cambridge Analytica, accessed and harvested 87 million profiles. It was involved in Brexit. It was involved in the Trump campaign.

Do you have any knowledge of it having involvement in Canadian politics?

Mr. Sami Khoury: I'm not aware of that.

Mr. Matthew Green: Okay.

You wouldn't know, then, that in 2016 the Liberal research bureau contracted Eunoia Technologies, under the founding member of Cambridge Analytica, Christopher Wylie, for a pilot project. He was the whistle-blower.

Are you aware of that at all?

Mr. Sami Khoury: No, I'm not aware of that.

Mr. Matthew Green: Would it concern you that the founding member of Cambridge Analytica, who was later involved in a significant scandal regarding the Trump campaign and Brexit, provided services in a contract with a Canadian political party, yet when we're doing a threat analysis, Facebook is never mentioned? How come?

Mr. Sami Khoury: In our role at the cyber centre, we want to make sure that we expose the threats and that we educate Canadians and Canadian organizations about the threats. We invite them to ask themselves the questions of how to protect—

Mr. Matthew Green: Respectfully, I'm just a working-class guy from Hamilton and it took me 10 minutes on Google to find that information. You're with the CSE. How is it that when you're doing a threat analysis of social media you don't find the threat of what I'll call algorithmic capitalism, the harvesting and sale of information for political purposes that would undermine democratic processes? I find that astonishing, to be quite frank with you, because when you talk about what's an acceptable level of risk, we've seen the impacts of Brexit and Trump.

Cambridge Analytica and Facebook, Mark Zuckerberg's company, had to testify in front of the U.S. Congress and had to pay fines in Europe for their interference in political processes, yet the only time we talk about threats, it's related to state-owned actors and not corporate actors, which are often hostile and, quite frankly, more mercenary when it comes to surveilling diaspora communities. I referenced the ways in which dictatorial regimes target their civilian populations here.

I will put this question to you. When you're doing your threat analysis, do you consider all of the other platforms and all of the other ways in which algorithmic capitalism can buy and sell our information and undermine our democratic institutions?

Mr. Sami Khoury: We definitely factor all of that into our threat assessment, but when we put out our advice and guidance, we pose a set of questions that we encourage Canadians and Canadian organizations, individually, to—

Mr. Matthew Green: I'm talking about the banning of an app on government devices. I'm not talking about your PR stuff with the public. I'm not interested in that.

We're here today on a very specific topic, which, for me, is why we're banning one social media outlet and not all of them. Would you not agree that Facebook, Twitter and Instagram also contain significant ways in which they scrape our data, control our likes, funnel us into different news streams, create echo chambers and, ultimately, create profiles on us?

Is that not correct?

● (1630)

The Chair: We need a quick answer.

Mr. Sami Khoury: Mr. Chair, if you share information, that can potentially contribute to the data-mining exercise of whoever is at the other end of that data leak.

The Chair: Thank you, Mr. Green.

Thank you, Mr. Khoury.

That concludes our first round of questioning.

[*Translation*]

Mr. Gourde, you have five minutes.

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

I want to thank the witnesses for being here. We rarely have the opportunity to welcome witnesses with such significant responsibilities as these. Thank you for working to keep Canada secure.

I want to return to the issue of foreign interference during the 2019 and 2021 elections. Did your services have the capacity to detect interference during those elections?

Mr. Sami Khoury: I will begin and then my colleague can respond.

The role of the Canadian Centre for Cyber Security is to collaborate with Elections Canada to ensure that elections infrastructure is properly protected. That's what we did during the 2021 election.

Mr. Jacques Gourde: I'm trying to determine whether you had identified foreign interference, particularly messages on social media that didn't originate from a political party or a political entity, but rather that originated outside the country.

Mr. Sami Khoury: Our role is not to examine the content of messages exchanged. Our main role is to protect infrastructure.

Mr. Jacques Gourde: If I understand correctly, you didn't detect foreign interference. Had you done so, would you have been able to block that information? Would you have been able to say that the information constituted foreign interference and to not to consult it? Do you have the capacity to do that?

During the election, candidates noticed that there were messages coming out of nowhere. They could read them. If, during an election, Canadians can view those messages, but you're telling me that you can't, I have a problem. In principle, you're here to conduct surveillance. Tell me why you can't see those messages, but the average Canadian can.

Mr. Sami Khoury: I want to make a clarification. We don't view content because we don't have the mandate to do so. The role and mandate of the Canadian Centre for Cyber Security is to protect infrastructure and not to check content. Clearly, we're concerned with infrastructure security, but also with foreign interference. Our goal is to teach Canadians how to stay as informed as possible and where to get the most credible information. Generally speaking, that's our focus.

Mr. Jacques Gourde: Thank you.

On what date following the 2019 and 2021 elections were you made aware that there had been foreign interference during the election campaign?

Mr. Sami Khoury: Unfortunately, I don't remember the date. I apologize.

Mr. Jacques Gourde: Would Ms. Henderson know the answer?

[*English*]

Ms. Cherie Henderson: Maybe I can answer this question. Thank you.

First of all, I'm going to start by saying that foreign interference does not occur only during an election. Foreign interference occurs all the time, every day, and I think we have to bear that in mind, because when you start to look at an election, which is a finite time frame, you're not going to always catch the foreign interference that's happening at that point. We start watching what's happening every day with regard to the buildup to an election, and we are constantly monitoring to see if there is any type of foreign interference coming from a hostile state actor.

When you're looking at a specific time frame and you're dealing with perhaps a social media attack, it takes a very long time to be able to figure out where that actually came from. You don't just flip a switch and already get it back to the country it came from or the threat actor it came from. It takes a long time for the intelligence services to put that work together and to follow that train back.

Also, when you're looking at social media, we do not monitor social media. You don't want your national intelligence service to monitor all social media. We have to make sure that we know there's a threat there, and then it comes under our mandate.

[*Translation*]

Mr. Jacques Gourde: Thank you.

I have a final question. It's one thing to know the origin of the attack, but knowing that the attack can influence Canadians and that it's illegal because the message isn't coming from Elections Canada is another thing altogether. Canadians are used to taking part in the electoral process. When that kind of attack occurs, it should be detected and condemned, and there should be a way to indicate that it's an attack and that those kinds of messages from outside the country should be ignored. Is it possible to do that?

● (1635)

The Chair: I would ask the witnesses to provide a brief answer.

[*English*]

Ms. Cherie Henderson: We also have to guard freedom of speech. We have to educate across the board to make sure that we are guarding freedom of speech but also educating, at the same time, in regard to foreign interference. It's an extremely complex situation. It's not just determining that, yes, this came from a foreign state; we also have to make sure that it's actually causing an impact to our sovereignty and our national security. Then we start to educate across the broader sphere on that perspective.

The Chair: Thank you, Ms. Henderson.

[*Translation*]

Thank you, Mr. Gourde.

[*English*]

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

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

Thank you to our witnesses for joining us today. I too would like to thank you for the work you do to protect Canadians.

Ms. Henderson, in terms of what you talked a little bit about, I'm a father of a teen and a preteen. We're all concerned about the youth of this country. We've learned over time how foreign states like Russia will work for a long time to try to influence a generation of people. You also mentioned that there are efforts to influence a whole generation of people.

Is that same practice now being followed by some of these other hostile nations that you talked about, whether it be China, Russia, Iran or North Korea? Are they copycatting? Are there developments of other applications that you think are in development to do that type of influence, such as with TikTok? We're now looking at TikTok and all these other social media platforms that are even based out of North America but are used worldwide. Are you monitoring other developments of other applications that we may not know of?

Ms. Cherie Henderson: We don't necessarily monitor the development of social media platforms. It goes a little bit back to what I said earlier, that I would worry that we would focus on one specific platform or two specific platforms. I think it's really important to start to educate everybody on really good social media hygiene. I don't know if that's a phrase, but I'm going to call it that. I think it's fundamentally important that every individual takes responsibility for what they're actually sharing and is aware of the cost and the impact that could have on them.

Therefore, if people are being aware and careful, then even if there are other media platforms, they're already in a good state of mind. They're protecting themselves. It doesn't matter if there's another platform developed, because they already have, again, good social media hygiene practices.

Mr. Parm Bains: Thank you.

Mr. Khoury, the CSE also alerts the government to foreign activities that seek to undermine prosperity and security, including cyberthreats, espionage, terrorism and kidnappings. Is intelligence also gathered or collected from social media platforms for these kinds of things?

Mr. Sami Khoury: In my role as the head of the cyber centre, I'm here to share with you the threat landscape as we see it. That threat landscape is informed from a number of sources. Some of them are public sources and some of them are classified sources. In a sense, whenever we find something, we will distill it down and we will put it out there, regardless of what the source is.

Mr. Parm Bains: Okay.

Were you able to watch the committee meeting on October 18, when representatives from TikTok testified? If so, what did you think of their testimony? They felt they were being unfairly targeted. Did you find their testimony persuasive in relation to security, privacy and data concerns? Did you have any concerns about their use of information sharing between third parties?

Mr. Sami Khoury: Unfortunately, I did not watch the testimony on the date you indicated.

● (1640)

Mr. Parm Bains: Okay. We asked them several questions around third parties having access to information. They felt they were being unfairly targeted. Do you find that's a concern with someone like TikTok specifically and the ability of third parties to have shared information?

Mr. Sami Khoury: The concerns we have are these: Who has access to the data? Where does the data reside? How easy is it for the host nation to get access to the data? That is what we are asking. Everybody who uses a social media app should ask themselves those questions in order to be a better-informed user of social media. In the case of TikTok, if the data is hosted in China, that would be a concern, considering some of China's permissive laws for getting access to user data.

We want Canadians to ask those tough questions about security settings in order to be better-informed consumers.

The Chair: Thank you, Mr. Bains and Mr. Khoury.

[*Translation*]

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

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

Ms. Henderson, earlier, you said that it was important to educate people about the potential risks posed by social media. However, the average person doesn't know the location of the servers hosting our data or what the risks are. The committee is somewhat better informed, but the general public is in the dark. So, how do we educate them?

Ms. Cherie Henderson: Thank you for this extremely important question.

[*English*]

I think education needs to happen at all levels.

Again, I'm not a policy person. I'm a mother, and I would like to make sure my kids get educated at schools, in community centres and across the board. We need to start to have that greater engagement, but that's me speaking as a mother, not as a security officer.

I think we need to have that education piece, absolutely. It's fundamentally important.

[*Translation*]

Mr. René Villemure: You talked a great deal about foreign interference. Earlier, you said that you didn't want to target anyone in particular, but, in the minute and a half remaining, could you tell us what we, as a committee, should but don't already know about foreign interference?

The Chair: To whom are you putting your question, Mr. Villemure?

Mr. René Villemure: I'm still talking to Ms. Henderson.

[*English*]

Ms. Cherie Henderson: Foreign interference is something we have been looking at in the service. I've been in the service for 32 years. From the day I started, we've been investigating foreign interference. It's something that has been in our country for decades.

Canadians have become very complacent and comfortable in our environment. I think we need to become much more aware of what's going on around us. It's become much more prevalent with the advent of social media and the technology we're dealing with. We are at risk from the activities of hostile states. They are interested in undermining our sovereignty and our democratic institutions. It's fundamentally important to protect the national security and the future of our country. We must take the necessary precautions, with awareness and education, in order to protect ourselves and our systems moving forward.

[*Translation*]

Mr. René Villemure: Thank you.

[*English*]

The Chair: Mr. Green—from a working-class guy in Barrie to a working-class guy in Hamilton—you have two and a half minutes.

Mr. Matthew Green: I appreciate that. Thank you very much.

I want to go back to your public advisories, Mr. Khoury. You mentioned that you provide general advice about social media. I note that a January 2023 article by the CBC stated, “CSE hasn't issued an advisory against using TikTok”.

Have you, by this date, issued an advisory against using TikTok?

Mr. Sami Khoury: In our role, we don't issue advisories on specific apps. We share advice and guidance about social media in general.

Mr. Matthew Green: Was it your advice to the Treasury Board to ban TikTok when they were investigating this?

Mr. Sami Khoury: That is a decision of the CIO of Canada.

Mr. Matthew Green: You did not advise them to ban it.

● (1645)

Mr. Sami Khoury: We contribute to the input into the decision. We are part of the round table with Treasury Board.

Mr. Matthew Green: At any time, did you advise them to ban TikTok?

Mr. Sami Khoury: No.

Mr. Matthew Green: Thank you.

Mr. Madou, I noted that Ms. Henderson didn't have the answer to my question.

Was CSIS consulted when the government decided to ban TikTok?

Mr. Peter Madou (Director General, Intelligence Assessments, Canadian Security Intelligence Service): Not to my knowledge, no.

Mr. Matthew Green: Did you advise, at any time, that the government should ban TikTok from government phones?

Mr. Peter Madou: We provide advice to government on foreign interference in the general sense. I'm not aware of us advising, specifically, on this social media platform.

Mr. Matthew Green: I'm still struck that this one social media platform, given all of the controversies around all of the other ones, was targeted. It feels like it was a political decision, not an evidence-based decision. That's my opinion. It's not yours.

In terms of threats, you have the mandate to investigate threats to national security. How often does CSIS investigate activities on social media platforms as they relate to threats to national security, Mr. Madou?

Mr. Peter Madou: We investigate threat actors; we don't investigate social media platforms. Depending on how threat actors are evolving, we may have insight into what goes on a platform, but otherwise we investigate actors.

Mr. Matthew Green: How often do you detect a presence of foreign interference services on social media platforms?

The Chair: I'm sorry, Mr. Madou. If you could just speak a little bit closer to the microphone, it would help the interpreters.

Thank you. Go ahead.

Mr. Peter Madou: Thank you.

Can you just repeat the question?

Mr. Matthew Green: How often does CSIS detect a presence of foreign interference services or actors on social media platforms?

Mr. Peter Madou: I think detecting counter-narratives on social media platforms may be a common occurrence, but to link them specifically to a hostile threat actor is a bit more complex. I'm not sure how often that happens. We do know that threat actors do that—such as the PRC, Russia, or other hostile state actors, as my colleague mentioned—but I don't have a specific number for you.

Mr. Matthew Green: Thank you.

The Chair: Thank you, Mr. Green.

Mr. Kurek, you have three minutes, please. Go ahead.

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

Thanks to our witnesses for being here.

In the fallout of the October 7 attack on Israeli citizens, there was information shared by a terrorist organization that the Prime Minister, the foreign affairs minister, other members of the government, and other political parties shared: that the IDF had bombed a hospital. This spread rapid-fire on social media yet was deemed very quickly to be categorically false. Our Five Eyes allies knew that this was misinformation, but our government refused to retract it. That is an example.

Ms. Henderson, can you share how that sort of action of the government would contribute to the erosion of trust, and share some of the challenges associated with social media and the influence that foreign states could have over the Canadian population?

Ms. Cherie Henderson: I'm not quite sure what you're asking me. I'm sorry.

Mr. Damien Kurek: When the Prime Minister and the Minister of Foreign Affairs refused to retract misinformation, they contributed to misinformation that spread rapidly online. I know it showed up in my feed, and it was forwarded to me by constituents as well.

When governments are slow to respond to combat misinformation, does that contribute to foreign state actors and the influence they may have over Canadians?

Ms. Cherie Henderson: How I would answer that would be to say that, in any situation, any foreign threat actor is always monitoring everything that's going on within a country of interest. They will pick up on any little piece of information, and they can magnify that into misinformation or disinformation in order to achieve their goal. They will continue to magnify that until they feel that the damage is done.

Mr. Damien Kurek: I appreciate that. Certainly, the need to combat misinformation is essential.

There's a disconnect in what TikTok has shared with this committee between the privacy settings that may be present on a phone and the grey side of social media where there may be unknown information that is collected.

In the 45 seconds I have left, I'm wondering, Ms. Henderson, if you can comment on how we can reconcile the disconnect that exists between what the social media companies are saying versus what we're hearing today and what has been reported in the media.

Ms. Cherie Henderson: The way I'm going to answer that is to indicate that there is always going to be, as you noted, a grey area. There is the policy and what the social media is collecting and engaging intentionally, such as—as they indicated—email addresses. However, as Mr. Khoury indicated earlier, it's not only the email address that you signed up with; everything else you are doing as an individual on that site is also data that can be collected. That's what we call, in many cases, big data. They will scrape all that big data off, and then they can do their data crunching.

That is where some of the danger comes in. That's where they can start to find the trends in the ways they can do the interference and the influence.

● (1650)

The Chair: Thank you, Ms. Henderson.

Thank you, Mr. Kurek.

Mr. Kelloway, you have three minutes to close things off.

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

Could I share my time with Pam Damoff, please, for the first 30 seconds?

Ms. Pam Damoff: I just need a few seconds. I wanted to clarify something that Mr. Kurek said.

The Canadian government reviewed the information on the hospital bombing on its own. The Prime Minister, quite emphatically, in the House of Commons and elsewhere, confirmed that it was not Israel that bombed the hospital. In fact, I remember the Conservative colleagues standing up and applauding when he said that in the House.

I want to make sure the record reflects that we did do our own investigation, Chair. We did, in fact, call out the misinformation.

I will turn it over to Mr. Kelloway.

Mr. Damien Kurek: I have a point of order.

Chair, I will note that this was five days after the information was shared.

The Chair: Go ahead, Mr. Kelloway. Thank you.

Mr. Mike Kelloway: Thank you, Mr. Chair, from one working-class person to another—I have to keep that trend going.

I really appreciate the work you do. I can't imagine the work that you do. I have so many questions, but in the period of time I have I couldn't possibly do it justice.

One particular item that keeps coming up is education. As an educator, I would love to unpack what that truly means. As you mentioned, the toothpaste may be out of the toothpaste container, but what do we do?

I'm going to try to crystallize it down to one basic thing. In terms of the radicalization of youth via TikTok or other platforms by foreign entities, can you drill down for us? Can you try to quantify how serious that is, to the best of your ability?

This is for any one of you or all three.

Ms. Cherie Henderson: I think it's a very serious problem.

These aren't going to be hostile states; these are hostile terrorist organizations. These individuals will be sitting in another country. They are out there monitoring social media, creating their own websites and looking for youth. They are looking for those individuals who perhaps are on their own, sitting in their room on their computer exploring and trying to answer questions. They are very vulnerable. Then those individuals pick up and they build a relationship.

Traditionally, in the espionage world, we used to call that creating a honey pot. You attract these individuals to come to you. That's what they do. Once they have these individuals, they continue to work on them. They continue to give them media pictures. They build that extremist ideology and they mould that young mind.

That's what I'm very worried about, because I think we have a lot of very vulnerable youth at this time and a lot of very hostile actors who are willing to take advantage of those children.

Mr. Mike Kelloway: Do I have much time?

The Chair: I think we can end on that point, if that's okay, Mr. Kelloway. I think it was a good point to make.

Mr. Mike Kelloway: That would be fine.

Thank you, Mr. Chair. I appreciate it.

The Chair: I don't know whom to direct this question to. I would probably direct it to Mr. Khoury.

One thing we haven't touched on yet is the impact of artificial intelligence and bot farms in the whole scheme of social media and the impact this may have going forward. How concerned should we be with the potential that AI and bot farms will be influencing not just young people, but all Canadians going forward?

Mr. Sami Khoury: We're definitely concerned about misuse of artificial intelligence. Artificial intelligence comes with opportunities, but also with challenges. We know that artificial intelligence is often used to amplify misinformation. Part of the algorithmic nature of some of those tools is to amplify misinformation.

We're also concerned about information leakage through artificial intelligence when you interact online. We've put out some advice and guidance to Canadians on how to make use of some of the public tools that are out there in terms of artificial intelligence, on being aware of the threat that is inherent in the use of artificial intelligence and on how some countries or some states are trying to exploit AI algorithms for their benefit.

● (1655)

The Chair: It's changing rapidly. What's the centre doing to stay on top of this? How are you staying on top of this as AI evolves? It changes rapidly and has a tremendous impact on the future. What are you doing about that?

Mr. Sami Khoury: We're doing a number of things. One is our own internal research on what the state of the art is in terms of what AI is up to these days. From a government perspective, we're also working closely with Treasury Board to ensure that it provides some guidance to the rest of the government departments on how to use those tools with informed advice. Beyond government, we've put out some publications. We talk. We offer speaking opportunities to inform about the threat that comes with AI.

Absolutely, there are opportunities, but we also know that the flip side of that opportunity is potentially a challenge or a threat.

The Chair: Thank you, Mr. Khoury, Ms. Henderson and Mr. Madou, for appearing before the committee. On behalf of the committee, I want to thank you for your service on behalf of Canadians.

We're going to suspend for a minute, and then come back with our next witness. We will need some time for committee business, probably about five minutes. I know we've scheduled 15 minutes, so we should have enough time to ask questions and have them answered.

We are going to suspend for a minute.

Thank you, everyone.

● (1655)

(Pause)

● (1700)

The Chair: Welcome back, everyone.

We are going to start the second part of our meeting today.

From the Privacy and Access Council of Canada, I'd like to welcome Sharon Polsky, president.

Ms. Polsky, you have five minutes to address the committee. Please go ahead.

Ms. Sharon Polsky (President, Privacy and Access Council of Canada): Thank you very much.

Thank you for inviting me to share some views about whether, and how, social media can undermine privacy, safety, security and democracy.

I am Sharon Polsky, president of the Privacy and Access Council of Canada, which is an independent, non-profit, non-partisan organization that is not funded by government or industry. It has members in the public and private sector who routinely use social media in their personal and professional lives.

Many can recall when Google mail was introduced. It was a brilliant marketing manoeuvre that preyed on human nature. Only the chosen few who were selected to have an account could have one. The invitation accorded those few people special status among their peers. This tactic and the media attention created demand. There was no talk about downsides, risk or privacy. People just wanted to have that Google account. It was simple psychology that showed how easily people can be manipulated.

Since then, we have seen countless examples of big tech manipulating us to share the most intimate details of our existence online. Social media continues to leverage human nature, and the lucrative data broker industry is the biggest beneficiary, other than those who would manipulate us for their own benefit, whether they're companies, political parties or governments. With recent geopolitical events, it's easy to think that what people post to social media might be used to coerce, extort or manipulate, but crediting social media alone, or social media from one country or another, is short-sighted.

Online risks reflect society and come from many sources, including familiar communication and collaboration tools that many in this room probably use most days. Every one of them is a real and constant threat. Zoom, Teams, Slack, Facebook and the rest are all foreign.

It's no secret that many companies scrape data and justify their actions by saying they consider the information to be public because their AI systems were able to find it on the web. Maybe the secure location where you posted personal or confidential information, or the Ontario hospital you visited recently, has been breached and now your health condition or sensitive conversations are being sold on the dark web.

If the concern is that people who use social media might disclose information that could make them politically sensitive and at greater risk of being influenced, I look to the recording we hear every time we call our cellphone provider or most other companies that says, “This call will be recorded for training”, which typically means the training of artificial intelligence systems through machine learning. The human side of that training is done in countries around the world by individuals who have access to your sensitive information.

A Finnish tech firm recently started using prison labour to do data labelling. It goes on and on. We have no choice whether the labelling is done by someone in Alberta or in Albania. There is no control over it and there is nothing stopping a company or a government from purchasing information, because it is available largely through the data broker system. It is widely available internationally. I could go on and on.

Yes, certainly education is important. Computers have been on desktops for almost half a century. The education is not there yet, as we see big tech investing tens of billions of dollars a year in objecting to and undermining efforts to regulate the industry, with the claim that it will undermine innovation. It's a red herring that's been disproven many times throughout history.

We see dating sites that people use routinely, which are wonderful for a social life, but when things like the Canadian dating site Ashley Madison are breached, I dare say that many of their customers become politically sensitive.

● (1705)

If children or adults go on any website, usually, before they even see the results, the fact that they have been there—whether it's for mental health, addiction or medical counselling.... That website has already secretly been transmitted to the likes of Facebook and data brokers.

This isn't something Bill C-27 is going to fix, or any of the other legislation. In fact, most of the laws being introduced here and abroad will make the situation much worse for everybody, including children—especially children.

I am happy to take your questions. This is a massive endeavour, and I commend you all.

The Chair: Thank you, Ms. Polsky. I'm sure our members have lots of questions for you. You will be the only one answering them, so here we go.

Mr. Kurek, you have six minutes. Go ahead, please.

Mr. Damien Kurek: Thanks, Mr. Chair.

Thank you very much, and welcome back to our committee.

One of the big challenges we face is this. When somebody downloads an app, they click a check mark for terms and conditions. There's education, increasingly, about what should or shouldn't be posted on social media. However, there's this grey world out there as to what information is actually being harvested or accessed—location and otherwise. In fact, it was this committee that looked into the fact that cellphone location information was shared with the government during the COVID-19 pandemic. It detailed people's trips to liquor stores, grocery stores and other public places.

How do we reconcile with this now "big data" world, where somebody downloads an app and checks a box, and all of a sudden their information goes to something we don't really understand? What are the impacts of where that data is going?

Ms. Sharon Polsky: It's a terrific question, especially considering that previous witnesses in this committee, from CSE and CSIS, repeatedly said it is up to the consumer, including children, to read the privacy policy and understand what is going on. A lot of my colleagues and members of the Privacy and Access Council of Canada don't get it. They don't understand it. How can we reasonably expect children or anybody else to? I live this stuff. Most people don't.

How does it happen? Largely, it's foreign companies. Our laws are obsolete, ineffective and poorly enforced. They do it because they can.

● (1710)

Mr. Damien Kurek: Are we seeing the gaps you're highlighting? Can you point to examples in Canada where that's being leveraged by foreign state actors, or by other entities that try to do Canadians harm? Can you point to examples and say, "That's where we're seeing the consequences of this playing out in real time"?

Ms. Sharon Polsky: I think it is pervasive.

Also, in the last half-hour, it took me a few minutes to find the birthdays of all but three members of this committee. I wish you an advance "happy birthday" for next week.

Mr. Damien Kurek: Thank you for that.

Ms. Sharon Polsky: It's very easy. Our information is out there, even if we put out bogus information. You can imagine what my children go through. They have their online birthdays. On their real birthdays, their friends say, "happy birthday" and the algorithms pick up on that. The algorithms detect, by the volume of greetings on the real date, that it's the real birthday, along with the other information amassed through this hidden data broker system, where our information is traded, sold and bid on instantly.

The minutiae of our lives are available globally for sale.

Mr. Damien Kurek: I appreciate that, and thanks for the birthday wishes. I'm certainly much younger than I look.

The thing that triggered this study was largely the issue of TikTok and the government banning it on government mobile devices. We saw, just a number of weeks ago, the government ban WeChat, which has certainly far more direct connections with the Communist dictatorship in Beijing. Those are two examples that have made headlines and that the government has taken action on, but we saw a weather app being one of the apps selling data, which the government purchased over the course of the COVID-19 pandemic.

More generally, can you provide your insight to the committee—in about a minute, if you can—about how we look at it from this perspective, the big picture, looking beyond just TikTok, WeChat or social media at the access we give entities to an incredible amount of information?

Ms. Sharon Polsky: I agree. It's not just a matter of one social media platform or another, one company, or one government or another. This is pervasive, and it's been growing for a generation.

What do we do about it? How do we stop it?

Yes, it's education starting at the very youngest ages. Is it too late to put the genie back in the bottle? No. There is so much information about each of us floating out there that we don't even realize that we individually are at a loss. Corporately, people who are procurement officers, who know as much or as little as most people, are at the mercy of the vendors. They're not interested in your privacy. They're interested in their commission, their bottom line and their shareholders benefiting.

Mr. Damien Kurek: I am out of time, so I'm going to ask you for a follow-up with some information. Would you be able to provide to this committee some specific recommendations—and we're talking largely about the impact this has on children—that this committee could make in terms of being able to address this, specifically with children but also the much larger societal impact of this?

I don't have time for you to answer that question, but hopefully you can provide that to the committee at a later date.

Ms. Sharon Polsky: I'd be happy to.

The Chair: Thank you. That's a good request.

Mr. Ehsassi, you have six minutes. Go ahead, please.

Mr. Ali Ehsassi (Willowdale, Lib.): Thank you, Mr. Chair.

Thank you, Ms. Polsky. That was very helpful.

I have a few questions.

We had Mr. David Lieber, who is the head of privacy public policy for the Americas for TikTok, testify before our committee. I was just wondering if you had a chance to review that testimony, by any chance.

● (1715)

Ms. Sharon Polsky: I read some of the written record, yes.

Mr. Ali Ehsassi: Was it misleading, in your opinion?

Ms. Sharon Polsky: No. Was it a complete, thorough, fulsome answer? I don't know, but from my experience—keeping in mind that I'm the president of the Privacy and Access Council of Canada, that I've been a privacy adviser for about 30 years, and that I've been inside a lot of organizations and have seen a lot of things—very often, the language in testimony, in media reports and in so-called privacy policies doesn't give the full story. We'll collect your information and share it with our partners and affiliates, but with whom, when, where in the world and for what purpose?

Mr. Ali Ehsassi: One of the things he did say, which struck me as somewhat odd, was that no one has anything to worry about because we are subject to Canadian law. Is that any comfort? If they have data and, as you were suggesting, they're sending it out to Albania or what have you, even if you're subject to Canadian law, I don't think there's much we can do, is there?

Ms. Sharon Polsky: As lawmakers, one thing you could do is not enact Bill C-27, because that's not going to make it better; it's going to make it worse.

What can we do? Is PIPEDA a comfort? No, it is not, because it's not sufficient, as Jennifer Stoddart said when she was in the final days of her role as commissioner. It could use some more teeth. How many years ago was that? It still needs some more teeth. Sure, Canadian organizations are responsible for the proper collection, use, disclosure and all the rest of it under PIPEDA, but when the information goes offshore, they lose control of it. We as Canadians have no recourse when our information is in a foreign nation and goes into the wind, or when we see things that breach our privacy, whether from Equifax, Meta, Google or any other organization.

One commission or another somewhere in the world hammers them with a multi-million dollar fine or hundreds of millions of dollars as a fine. They put it in their financial report as a line item, and it reduces their tax liability—that's sweet, on to the next. That's all. It's lunch money to them. It's to the company, not an individual.

Mr. Ali Ehsassi: Thank you for that.

Something else we should be very much concerned about is ransomware. Could you talk about the intersectionality between these social apps and the information that's obtained and then leveraged against consumers?

Ms. Sharon Polsky: I think that ransomware, like so many problems we have online, is a reflection of society. It is the same type of crime that was committed before the Internet. The Internet is a tool that allows the perpetrators to commit these crimes in greater numbers, with greater efficiency and cost efficiency from their side, with greater returns. That's terrific, but it's no different. It's really no different.

The problem is education, again. You can have the best technology, the greatest security, but if somebody doesn't have the courage to question the boss or to call up the president and say, “Excuse me, ma'am, but did you actually send this?” or if they don't have the curiosity or the skepticism, especially nowadays, to question what is presented in their email—and I'm sure they act in good faith—and if they click the wrong thing, that opens the entire organization up to ransomware and to problems.

The organization can recover, but what about all the individuals whose personal information has now been compromised? In the case of Equifax, there were 146 million Americans, and the payout, the negotiated settlement, the fine.... I remember Kevin Mitnick, when he was still alive, on LinkedIn showing the cheque he got for $5.42. That was supposed to help him recover. In Canada, the Canadians who were affected got one or two years of credit monitoring that was administered through Equifax's American organization.

● (1720)

Mr. Ali Ehsassi: My last question is this: Given that you probably have had the opportunity to look at various jurisdictions, what jurisdiction would you say does the best job of ensuring that privacy rights are protected?

Ms. Sharon Polsky: At this point, I would say it's the EU, because of the GDPR and because, at the very last minute, they put the brakes on a piece of legislation that would have required, basically, encryption to be broken to facilitate the ability of the police to find the predators. The police do that now without the encryption back doors.

The Chair: Thank you, Ms. Polsky and Mr. Ehsassi.

[*Translation*]

Mr. Villemure is next.

[*English*]

Do you have your earpiece in, Ms. Polsky?

Ms. Sharon Polsky: I do.

Thank you.

The Chair: That's wonderful.

[*Translation*]

Mr. Villemure, you have six minutes.

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

I too want to wish my colleague Mr. Kurek a happy birthday.

Good day, Ms. Polsky. It's a pleasure to have you here.

How would you describe the behaviour of social media platforms in terms of privacy protection?

[*English*]

Ms. Sharon Polsky: I would say they are self-interested, because they are for-profit organizations. They do what they have to in order to improve their bottom line and to provide the greatest return possible to their investors and shareholders.

[*Translation*]

Mr. René Villemure: Are they all the same, or are there some that are better than others?

[*English*]

Ms. Sharon Polsky: I think there are some that are better. They do take a greater interest in individuals' privacy. I could name the Tor Project, Signal, and Proton. These are the three that come to mind. They're not particularly social media platforms, but they are certainly communications tools that don't take any information, any metadata, anything. They don't keep it. That provides much greater security. As well, their encryption technology is much stronger.

[*Translation*]

Mr. René Villemure: In terms of privacy protection, social media platforms are all the same, meaning they aren't very good. Is that correct?

[*English*]

Ms. Sharon Polsky: That's a very difficult one, because each one of them has its own interests at heart. They collect the information and provide advertisers with the opportunity to reach our eyeballs. I don't know that any of them is really interested in our privacy.

[*Translation*]

Mr. René Villemure: On that subject, could you comment on surveillance capitalization and tell us what a committee such as ours can do to counter its impact?

[*English*]

Ms. Sharon Polsky: “Surveillance capitalism”, the term that Shoshana Zuboff coined, is a wonderful term. We could also call it “surveillance economy”, because nowadays much of our economy is based on surveillance in one way or another, whether we realize it or not.

What can be done? Before a drug is allowed to be sold in Canada, before a vehicle is allowed to be sold and licensed in Canada, and a lot of other products, they have to be tested by an independent Canadian authority to make sure they are fit for purpose and safe. I think the same thing has to apply to the technology we all use every day, which is now being sold by self-interested corporations. That all fosters the surveillance economy.

The only way of pulling back from having our information used continuously as fodder for surveillance.... Spin doctors say, “Well, everybody is okay with it because they keep giving their information”, despite the fact that we have very little option or no way of opting out. It's up to our government to regulate it, despite the objections of big tech.

● (1725)

[*Translation*]

Mr. René Villemure: You said earlier that, despite the efforts expended on C-27, it did nothing to protect us from those kinds of invasions of privacy, is that not correct?

[*English*]

Ms. Sharon Polsky: Well, I think it's a step backwards from what we now have in PIPEDA. First of all, the first word is “consumer”—the consumer privacy protection act—labelling us all as consumers. We are commodities, with our information to be commoditized.

It provides a private right of action once we complain to the commissioner, who is—like most of them—chronically underfunded. Once they finally get around to assigning the file, investigating, deciding and determining, it will go to a new tribunal, which I expect will have to at least review this, if not provide a fulsome reinvestigation. If the tribunal agrees with the commissioner that a fine is in order, then the offending company has the right to take it to court.

How many years will that take? Once they have exhausted their legal recourse, you and I get to advance our private right of action. We then pay another lawyer and go through another 7-10 years.

[*Translation*]

Mr. René Villemure: So it isn't very useful.

You mentioned earlier that merely going to a web site, before even clicking on the consent form, constituted data. Could you tell us a bit more about that?

[*English*]

Ms. Sharon Polsky: Yes, this is a feature that.... I've found that in a lot of organizations, the people who create the websites don't talk to the people in the privacy office, shall we say. It's the old story that we'll put in all of these wonderful tools that can collect information, and it's really neat to say, “Hey, we can maybe do something with it in the future”, without knowing—because of lack of education—that they are overcollecting. The way it works is similar to a cookie. Before you even see the website you have called up, the fact that you are there has already been transmitted to Facebook and data brokers.

[*Translation*]

The Chair: Thank you, Mr. Villemure and Ms. Polsky.

[*English*]

Next, we have Mr. Green, for six minutes.

Go ahead, please.

Mr. Matthew Green: Thank you.

I certainly appreciate your quite right analysis of the consumer as the commodity. I think this absolutely underscores most of what we're talking about here.

Were you here during the previous panel? If you were, you would have noted that in my lines of questioning I brought up quite frequently the notion that there isn't one bogeyman in this scenario, but in fact all platforms are engaged in this type of surveillance capitalism. Whether or not a foreign state actor has direct access via ByteDance, or another dictatorial regime purchases it as the highest bidder from another, fundamentally there isn't really a difference. They have the data.

Would you agree with that analysis?

Ms. Sharon Polsky: Absolutely. Our information is being sold, traded and bid on in real time. We don't know it and we can't say, no, don't do that, because we have no idea who is bidding on our information. We don't have a direct relationship with them. We have no recourse. Our information is gone.

Mr. Matthew Green: On that, I want to talk about the recourse. You mentioned the teeth that you would like to see in legislation.

With specificity, could you just take a moment and reflect on the types of teeth you would like to see in a proposed legislation that would deal with privacy in a more fulsome way?

Ms. Sharon Polsky: I can give you a very quick example.

The way companies now are fined, but not the individuals, is meaningless. By contrast, after the Enron scandal, 20 to 25 years ago, the United States passed the SOX legislation. The complete name is the Sarbanes-Oxley Act of 2002. It said very simply that the person at the head of the organization is responsible for everything in the financial statement. If things go sideways, they personally face multi-million dollar fines and jail time. Companies around the world, including Canada, scrambled to make sure that they were SOX-compliant. We need the same thing.

● (1730)

Mr. Matthew Green: Is it your assertion that when someone is not granting full information and full consent when engaging in an app or a platform, this is a type of fraud committed by the company and therefore should have a criminal liability to it?

Ms. Sharon Polsky: I wouldn't go so far as saying it's fraudulent, but it's perhaps misleading. It's permitted under the current legislation and under Bill C-27, which is going to maintain the status quo of the same vague consent. That's not going to improve the privacy.

Mr. Matthew Green: Here's a chance for you now to address that specific consent clause.

I would say that if you're not entering with full understanding, you can't consent. If you're downloading an app for a certain use and your use of that app is then sold to third parties that you don't know about and the real purpose of the app.... I reference Cambridge Analytica. They had your life in data. I can't remember the exact name of the app where they scraped all this information. I would say it's fraud. You don't have to say that, but I would say it's a fraudulent engagement of the consumer.

As it relates to consent, again, could you just provide, with specificity, the types of explicit consent you would like to see so that people who engage with these platforms would have full prior knowledge of what it is they are engaging in?

Ms. Sharon Polsky: Okay. There are two things you're talking about here, I think.

One is that the companies or organizations that are supposed to obtain our informed consent at the time of or prior to collecting our personal information acknowledge—as did Mark Zuckerberg before Congress—that few people read these privacy policies. This, to me, says they are collecting our personal information knowing that nobody reads the privacy policy. Therefore, it is not informed consent. They are in violation of our privacy legislation, the GDPR and others.

What to do about it? Turn it around. Stop allowing the organizations to be in control. Turn it around so that we each have the ability to—

Mr. Matthew Green: Opt in rather than opt out.

Ms. Sharon Polsky: No, it's more than just opting in or opting out. Interrogate the company. Make it so that there is an index of companies where consumers can go and see how a company complies with the legislation. If one company does it in a way that is better than another, the consumer can make a choice. I allow my information to be used by your company for a certain purpose. I get a receipt. There is a record of it that I am in control of and not the company.

Mr. Matthew Green: That's interesting. I appreciate that.

I think the last study you were here for, sometime back, was about surveillance on phones, with the RCMP.

Ms. Sharon Polsky: Spyware.

Mr. Matthew Green: Yes. Here we are. In a lot of ways, whether it's governments using these devices or corporations using these kinds of device applications, it's spyware. Would you agree with the assessment that social media apps are a form of spyware?

Ms. Sharon Polsky: Absolutely.

Mr. Matthew Green: Would you care to expand on that?

The Chair: Please respond very quickly.

Ms. Sharon Polsky: I have a challenge with that sometimes. There's a lot, as I said, to discuss.

It's the granularity of the information they collect about us—usually without our knowing about it—such as the ride-sharing app we use that records the precise geolocation and the time of day. They can use it for their own purposes. Whom is that given to, and what assumptions can be drawn from that or any other information?

It is effectively spying on us. I agree.

The Chair: Thank you, Ms. Polsky.

[*Translation*]

Mr. Gourde for five minutes.

Mr. Jacques Gourde: Thank you, Mr. Chair.

I want to thank the witnesses. Their statements and those of the previous witnesses have left me quite concerned.

We, as human beings, have become products. These major companies have created a profile for each of us based on our aspirations, what we buy and what we look at. That profile is then re-sold to companies wanting to sell us something.

It's my impression that it's already too late for my generation and all those currently using social media. I'm the proud grandfather of six grandchildren—soon to be seven—, who are too young to use social media. Should we be focusing on protecting the next generation?

● (1735)

[*English*]

Ms. Sharon Polsky: We're protecting the next generation, absolutely, but we're all fighting against well-funded big tech that insists everybody wants this. Nobody understands it. Well, a few people understand it well enough to object to what it is doing to us.

Things have changed very quickly. I think it was in 2004 when a minister of the Canadian government was in the hot seat because it had been discovered by the media that the government was collecting 2,000 bits of information about each of the 33.7 million Canadians when there were some 31 million Canadians. People reacted quickly and vocally. The minister said, “Never mind. We've given the information back”—how you do that with electronic data, I don't know—and they apparently disbanded it.

That very quickly changed. Instead of dealing with one government department or another, now we deal with government, and the government says it owns our information. The whole concept of public policy has shifted. I dare say that if there is a genuine interest in preserving and protecting children, privacy and future generations, there needs to be some serious thought given to actually doing that. Studies are wonderful, but action has to be taken very quickly.

[*Translation*]

Mr. Jacques Gourde: Is this current quest for information on all individuals a breach of our individual freedoms.

[*English*]

Ms. Sharon Polsky: Is it a threat to our liberty? Absolutely. It's too easy for any organization to use the information that has been amassed about us to sway our views, to sway views of public policy, government, legislators, teachers, institutions. It's absolutely a threat to democracy and civil liberties—human rights. Artificial intelligence is going to make it even worse, unless there is effective, strong regulation to protect individuals, not just to foster commerce.

[*Translation*]

Mr. Jacques Gourde: Thank you very much.

The Chair: Thank you, Mr. Gourde.

[*English*]

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

Ms. Pam Damoff: Thank you, Chair.

Thank you so much for being with us today and bringing your vast knowledge to our committee.

I want to go back to youth. Earlier, when we had CSIS and CSE here, I said that when TikTok appeared, they said the only thing they collect is an email address. They make sure that young people give them their birthdate and everything is just tickety-boo. They don't have any young people who shouldn't be on there. I challenged them at the time.

I wonder if you could just share with us a little bit. Young people sign up. They give an email address. How much more information are TikTok and Instagram, which are the two popular ones with young people, gathering and how are they gathering it? Is it of concern to you?

Ms. Sharon Polsky: I have not investigated either of those companies closely enough to know what they gather, but in more general terms, companies do gather that information.

Typically—and keep in mind that we're told to respect authority and to give a straight answer when asked a question—people give their real information. It doesn't occur to them to give a made-up name or a made-up birthday or to use an email address that is a throwaway or that hides their real email address. They use their email address, and that gets connected in the background by the data brokers. It's a huge concern.

As for how to identify whether somebody is providing their real age or not, there are a lot of companies that are selling this service. They will collect your government photo ID and they will verify it. They amass that information, and that is another threat. On legislation, I know that Canada is thinking about the same thing that the U.K. and the EU have been thinking about—or, in the U.K.'s case, it has been enacted—and that is requiring organizations to collect that information. That is a huge threat.

● (1740)

Ms. Pam Damoff: To go back to the young people, we haven't talked at all about apps and filters. I remember that a few years ago there was a thing going around where you could download an app onto your phone that would show you what you would look like in 20 years. I remember all kinds of people downloading that app and uploading their pictures—it's fun to share these pictures—and then it turns out that the company was based in China and that information was actually not secure.

I often see young people who have downloaded filters that can turn them into a Disney character or whatever the filter app might be. I'm just wondering if you have concerns about those kinds of things that appear to be fun but are in fact quite dangerous in terms of the information you're sharing.

Ms. Sharon Polsky: I think they're very much like the questions you get: What's your favourite dog, your favourite animal or your favourite colour, or if you were a car, what would you be? These are all subtle ways of gathering information about people and their psychological makeup and their preferences. You don't know who's collecting it and what they're going to use that information for. It's a huge concern, absolutely.

Ms. Pam Damoff: I hadn't thought of that, but quite often on Facebook, it will say “take this quiz”: What city were you born in and where did you go to school? Often, people don't look at their security settings to see whom they're sharing with, and it ends up being public. You've given people all the information they need to breach your security, because those are often the answers that you use for questions when you have your credit cards or banking information.

How do we educate the public, though? There's an onus on the companies, but there's also an onus on Canadians—and around the world, but we'll focus on Canada. How do we educate Canadians to be more aware of what they're sharing online?

Ms. Sharon Polsky: There are places, well-funded organizations, that promote education, but it's a drop in the bucket. I think it's a matter of public policy to require.... I realize this is not a federal jurisdiction thing, but I'm sure the federal government could have some influence, perhaps, with its provincial and territorial colleagues, to say, “Include this in the mandatory curriculum, from pre-kindergarten.”

Ms. Pam Damoff: I know that's my time.

I used to be on the public safety committee, and digital literacy is something that we've asked for many times in terms of getting it into the schools.

Thanks for being generous with your time, Chair.

The Chair: I'm probably the most generous guy you'll ever meet.

Some hon. members: Oh, oh!

The Chair: What are you laughing at? Just look up my profile on Facebook.

[*Translation*]

Mr. Villemure for two and a half minutes.

Mr. René Villemure: Thank you to our very generous chair.

Ms. Polsky, earlier, my colleague Matthew Green and you were discussing improvements needed to ensure people aren't trapped and without recourse once they give their consent. In my opinion, many elements of that discussion are extremely interesting. Could you tell us more?

[*English*]

Ms. Sharon Polsky: I've lost the interpretation.

[*Translation*]

The Chair: We've lost interpretation, Mr. Villemure.

[*English*]

Ms. Polsky, make sure you're on the right channel. You want English.

Ms. Sharon Polsky: I'm on English, but it faded away. I couldn't hear the translation for the entire question.

The Chair: Okay.

[*Translation*]

Mr. Villemure, I paused the clock on your time. You may ask your question again. We'll make sure that Ms. Polsky is able to understand it. Please start over.

● (1745)

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

Ms. Polsky, you were talking with my colleague Mr. Green, who will speak after me. You both listed solutions to prevent people from being trapped without any recourse on the issue of consent. I'd like you to speak more about possible solutions, which I find quite interesting.

[*English*]

Ms. Sharon Polsky: One of the things we see in existing Canadian and foreign legislation is consent that has no granularity. You have to consent to the organization collecting information from you and about you. It'll be shared with its business partners and affiliates. You don't know who those are, where in the world they are or what they're going to do with it.

Bill C-27 maintains the status quo, except it's going to have to be in simple, non-legalese English. It doesn't change anything. It's not granular. We need granularity.

Actually, the Quebec government has a new piece of legislation that was enacted about a year ago. The consent portion of it came into effect in September this year. It is better. It's not what it needs to be. It still gives the organizations the reins.

We need to turn it around so that the organizations are compelled to comply with legislation and be rated on their compliance by an independent organization that creates a publicly available index, if you will. We can then all go to this index and determine whether or not we want to deal with an organization based on its compliance with the legislation. It is then up to us to give our consent.

[*Translation*]

Mr. René Villemure: I'm going to use my final 10 seconds to summarize your opinion that we need privacy legislation similar to the Sarbanes-Oxley act, a driver for this kind of activity. I'm very interested in the connection to this legislation. Could you clarify your thoughts on the matter or send us documents in writing?

[*English*]

Ms. Sharon Polsky: I'd be happy to send more information. I'm working with colleagues who are developing an international standard and a facility to do just what I've been describing. It turns it around, puts us in the driver's seat and compels organizations to comply with legislation.

That's important, considering there are still a lot of them in Canada that have yet to comply fully or at all with PIPEDA, 20 years later.

[*Translation*]

The Chair: Thank you, Mr. Villemure and Ms. Polsky.

[*English*]

Mr. Green, you have two minutes and 52 seconds. Go ahead, sir.

Mr. Matthew Green: I appreciate the reverse onus. I agree. However, if compliance is an issue, why have this rating mechanism that you've imagined, instead of just hard regulation and hard compliance that would have some kind of teeth, with fines that meet a disincentive or, worse, with criminal culpability?

Ms. Sharon Polsky: Go at it with both prongs, so that the organizations have to comply. Think of it as what Ralph Nader did long ago with the auto industry. Some people called it public shaming.

If you don't know how an organization is complying, whether it's complying or to what extent it's complying, you're in the dark.

Mr. Matthew Green: I would agree.

Ms. Sharon Polsky: Make it so that it has to publicly fess up.

Mr. Matthew Green: You mentioned that Bill C-27 is the status quo, and I appreciate that. It's basically making them use plain English, but it's still putting the onus on the person rather than the corporation.

Will more legislation be needed to properly regulate social media platforms, in your opinion?

Ms. Sharon Polsky: I think there are an awful lot of laws already on our books that address the societal problems and the human nature problems that we see online and in social media. I don't know that having more laws—certainly, not more bad laws—is going to improve anything, so the answer is no.

Look at what we already have and enforce that.

Mr. Matthew Green: Then you think that what we have is sufficient.

Ms. Sharon Polsky: If the people in a position to enforce had the authority to enforce the laws, yes. Now we have people who have the responsibility, but not enough authority or funding.

● (1750)

Mr. Matthew Green: To be clear, increasing the authority for oversight over these platforms, with teeth that include a reverse onus on the corporation, as well as regulation and/or public shaming, would be your recommendation to provide better oversight for social media platforms.

Ms. Sharon Polsky: Yes, but I would challenge you on your reference to “a reverse onus on the corporation”. No, it's an obligation they already face under legislation. Make them comply.

Mr. Matthew Green: I should say, “reverse the onus”—

Ms. Sharon Polsky: Yes, reverse it. Thank you.

Mr. Matthew Green: —because presently the status quo is that the onus is on the person who could not possibly consent or be informed about where their data goes. You're suggesting—quite rightly, I would add, in my opinion—that that be placed on the people who create the algorithms, broker the information and ultimately profit from it.

Ms. Sharon Polsky: That's right. They monetize our information. They should be the ones to prove that what they are foisting upon an unaware and unsuspecting public is safe and is not going to undermine privacy, security and national security.

Mr. Matthew Green: Thank you.

The Chair: Thank you, Mr. Green.

Thank you, Ms. Polsky, for appearing before the committee today. That concludes our second round of questioning. On behalf of Canadians, I'd like to thank you for the information you've provided and for your work as well.

We are going to suspend for a couple of minutes. We're going to return in camera. I expect it's going to be quick. We have a personnel issue that we need to discuss.

[*Proceedings continue in camera*]