HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

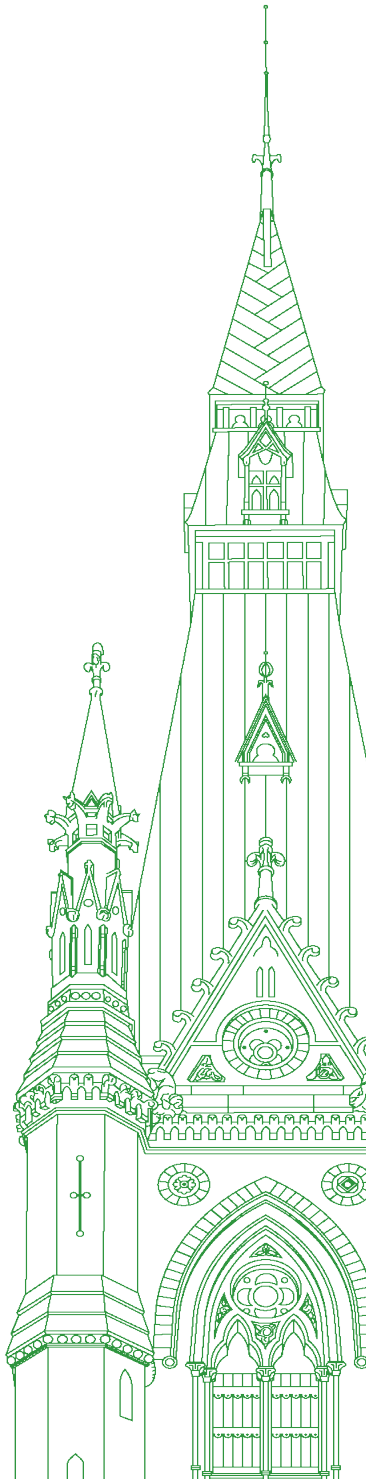
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 145

Thursday, December 12, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Thursday, December 12, 2024

● (1600)

[*English*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): I'm going to call the meeting to order.

[*Translation*]

Welcome to meeting number 145 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Tuesday, October 29, 2024, the committee is resuming its study of privacy breaches at the Canada Revenue Agency.

I would like to welcome our witnesses for the first hour of this meeting.

[*English*]

From H&R Block, I want to welcome Mr. Peter Davis, who is the associate vice-president of government and stakeholder relations.

Mr. Davis, welcome to committee. You have up to five minutes to address the committee, and then we'll be following that with questions.

Go ahead, sir.

Mr. Peter Davis (Associate Vice-President, Government and Stakeholder Relations, H&R Block Canada Inc.): Thank you very much, Mr. Chair.

Thank you, committee members, for the opportunity to appear on behalf of H&R Block Canada today. I appreciate the committee's patience and flexibility in accommodating my schedule.

This year, we at H&R Block Canada are proud to be celebrating our 60th anniversary of helping Canadians with their taxes and with receiving their benefits. Back in 1964, H&R Block Canada's first tax office was established in Toronto, and our national headquarters are proudly located in Calgary today. Throughout our 60 years in Canada, our company has grown to nearly 1,000 locations and 10,000 H&R Block Canada associates, serving Canadians in every corner of the country during tax season.

I'd like to reiterate some key points from our earlier November 15 statement and our December 6 submission to the committee.

Throughout our more than six decades of operation, H&R Block Canada has placed the utmost priority on ensuring the protection and privacy of our clients' tax information. H&R Block Canada is proud of our retail offices' privacy framework, which is among the best in Canada. We understand the important responsibilities and obligations that come with safeguarding Canadians' personal information, and we have robust security systems and processes in place to protect it.

Given H&R Block Canada's commitment to data privacy and security, when we became aware of the incident involving our e-file credentials, we immediately conducted a comprehensive internal investigation and concluded that H&R Block Canada's data, systems and software had not been compromised. We are also not aware of any impact to our clients.

I would also like to assure this committee that H&R Block Canada has never sent any Canadians' personal data, including pixels, to companies such as Google and Meta. While we are aware of past media reports in the U.S. regarding this issue, we can confirm that the pixel usage described in those reports does not apply to H&R Block Canada clients.

Allow me to take a moment to speak on behalf of our broader industry.

As co-chair of Tax-Filer Empowerment Canada, the national trade association for Canada's tax preparation and software industry, I believe it is important to articulate the critical role of industry tax software in helping to safeguard the personal information of Canadians. Tax software developed by industry for use by taxpayers directly or by tax professionals on behalf of their clients must undergo intense certification by the CRA each year in order to be approved for use by the public and to be authorized for the electronic filing of tax returns to the CRA. Tax software providers must also ensure that their products and services are compliant with Canadian privacy and data security legislation. These factors, along with industry innovation and ongoing investment to continuously enhance and evolve data security, afford Canadians many diverse industry options to choose from so that they can feel safe providing their personal information.

Diversification mitigates cybersecurity risks, as threat actors have to attempt to infiltrate several different secure IT systems, as opposed to just one system administered by the CRA. With this in mind, along with the fact that the CRA is a high-value target to threat actors and has experienced previous security breaches, the notion that taxpayers' information will be safer if it is solely controlled and managed by the CRA through automatic filing or any type of government tax filing does not have a credible basis.

Before we move to questions that committee members may have, I would like to raise this point. These proceedings are very likely being monitored by threat actors seeking opportunities to identify and exploit potential data security intelligence for criminal gain. As the largest assisted tax preparation company in Canada, H&R Block Canada closely monitors and defends against attempted cyber-threats on a regular basis. Accordingly, any statements we provide as an organization regarding cybersecurity must be careful not to reveal sensitive information that could give threat actors any intelligence to assist with their criminal activities. Further, we are bound by Canadian privacy legislation and H&R Block Canada's client privacy and data security policies to ensure that no personal information of Canadian taxpayers is disclosed.

Thank you again, Mr. Chair and committee members, for inviting me to appear today on behalf of H&R Block Canada. I am pleased to answer any questions that you may have, to the best of my ability.

The Chair: Thank you, Mr. Davis.

We're going to start with six-minute rounds of questioning.

Mr. Caputo is going to lead us.

Go ahead, Mr. Caputo.

Mr. Frank Caputo (Kamloops—Thompson—Cariboo, CPC): Thank you, Mr. Davis, for being here, and thank you for your opening statement.

What I took from that is that we're dealing with an obviously massive data privacy breach here. That's what really brings us to Parliament today.

Is it fair to say that it's your position that this was not on H&R Block and is solely on CRA?

Mr. Peter Davis: Thank you for the question.

As I mentioned in my statement and in earlier submissions to the committee, when H&R Block Canada was notified by CRA that there was a compromise of our e-file credentials, we immediately launched a comprehensive investigation. We left no stone unturned. Throughout the course of that investigation and upon its conclusion, there was no evidence to suggest that H&R Block Canada's systems, software or security apparatuses had been compromised in any way.

As to where this compromise may have taken place, H&R Block Canada can't say for sure, but we know that it was not within our organization.

● (1605)

Mr. Frank Caputo: Thank you.

Are you familiar with how things are done in the United States? In Canada, as I understand it, essentially, there isn't a lot of information sharing between H&R Block and CRA when it comes to cyber issues, but the United States does it a little bit differently.

Are you familiar with all of that?

Mr. Peter Davis: I am familiar only at a cursory level. I'm here in my capacity today representing H&R Block Canada and our operations here in Canada, but I am familiar with some high-level aspects of collaboration between IRS and the tax preparation industry in the United States, such as the security summit, which is an annual gathering of both the industry and the IRS to share best practices about cybersecurity and talk about potential threats, to the extent that's possible and appropriate.

Mr. Frank Caputo: You spoke about collaboration. Is it your view that the sort of collaboration you just described happens in Canada?

Mr. Peter Davis: It doesn't currently happen in Canada. It is something that our company and the industry have recommended to CRA in the past, and we continue to recommend that. To the extent possible, we would like to see more collaboration between the agency and the industry, to combat fraud and any other type of cybersecurity threats.

Mr. Frank Caputo: Do know how long you've been recommending greater collaboration with CRA to address these increasing cyber-threats?

Mr. Peter Davis: It has come up in industry conversations with CRA off and on over the last, I would say, two to three years, approximately.

Mr. Frank Caputo: Can I ask what the CRA's response has been?

Mr. Peter Davis: They have always expressed receptiveness to the idea. I think one of the challenges that CRA has communicated to us with that concept is how something like that can be put together and still respect Canadian data privacy legislation.

Our understanding is that CRA is looking into that and, hopefully, once we have a clearer picture of what may be possible, we can potentially explore moving that forward.

Mr. Frank Caputo: On behalf of H&R Block, do you see that as an impediment?

Mr. Peter Davis: Do I see what as an impediment?

Mr. Frank Caputo: I mean, what you just described. Do you see the protection of privacy as an impediment to greater collaboration? If that's CRA's issue, do you agree with them in that regard?

Mr. Peter Davis: I would say that, to the extent that it's preventing CRA from being able to collaborate where appropriate with industry and with our organization, then, yes, it would be an impediment.

Mr. Frank Caputo: Okay. In terms of the data breach, the information sharing and the cyber-threats that bring us here today, do you feel there was any area in which CRA did not act as quickly as it could have?

Mr. Peter Davis: I'm not in a position to answer that, given that we did not have a line of sight into CRA's investigation and most of the mitigating measures that they may have employed. I'm not able to answer that with any accuracy.

Mr. Frank Caputo: Do you feel that their communication with H&R Block was done in a timely manner?

Mr. Peter Davis: Yes, it was, in terms of notifying us when this incident may have began. That communication, I believe, did happen in an expedient manner.

Mr. Frank Caputo: Okay.

Mr. Chair, how much time do I have left?

The Chair: You have a minute and a half.

Mr. Frank Caputo: I want to get into that a little bit more.

What is your understanding of when the breaches came to light? When was H&R Block notified?

Mr. Peter Davis: I'm not able to disclose the exact date, just for security purposes, but we were notified in April of this year. Immediately upon being notified, we launched our investigation into our system, software and security apparatuses.

Mr. Frank Caputo: To the best of your knowledge, did any of your clients have any losses as a result of this?

Mr. Peter Davis: We are not aware of any impact to our clients as a result of this incident.

Mr. Frank Caputo: Do you know exactly how many clients were impacted by this?

Mr. Peter Davis: We do not know how many Canadians may have been impacted by this, no.

Mr. Frank Caputo: Do you even have an estimate?

Mr. Peter Davis: No, I have nothing that is based on anything factual.

● (1610)

Mr. Frank Caputo: Have you made safety recommendations to CRA based on what happened on your end?

Mr. Peter Davis: Yes, we provided a series of recommendations to CRA in August of this year. Our understanding is that CRA is continuing to review them, and we're looking forward to engaging with them as soon as we possibly can.

Mr. Frank Caputo: Has CRA given you an update as to whether or not they will be accepting them and where the progress is?

My concern is this. We're now in December. These were made in August. We don't want to be in a situation where we're here again. I'm just wondering—

The Chair: Mr. Caputo, I'm sorry, but your time is up.

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

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

Peter, it's nice to meet you today. Thanks for being here.

Some of the things that are asked might be things that were asked and phrased in different ways but are all going to be about the same topic.

In the letter you sent to our committee, H&R Block Canada said, “H&R Block Canada's data, systems, and software were not compromised”.

I'm interested in the codes that are assigned to your tax preparer offices. Tell the committee a little bit about your internal strategies and policies to ensure that there is security for those codes.

Mr. Peter Davis: I will attempt to answer that to the extent possible, given that I'm unable to share quite a few specifics in relation to this question. It does bump up against our security and client privacy policies.

What I can say is that e-file IDs are issued by CRA to tax preparer offices, and the expectation is that those IDs are treated with the utmost confidentiality.

Mr. Darren Fisher: Have you had any issues with those codes?

Mr. Peter Davis: No.

Mr. Darren Fisher: You've never had a leak of those codes.

Mr. Peter Davis: No.

Mr. Darren Fisher: How do you guarantee that your staff might not be the source of the leak that we're talking about today?

Mr. Peter Davis: That was part of the investigation that we undertook and, as I mentioned earlier, we left no stone unturned. We did a comprehensive review of just about everything that's related to e-file ID credentials and how they are used within our organization. There was no evidence to suggest that our staff were in any way involved or responsible for what took place.

Mr. Darren Fisher: When you're sourcing new staff, do you do criminal record checks and things like that?

Mr. Peter Davis: Yes, we do criminal background checks on all of our associates.

Mr. Darren Fisher: Do you do this for everyone who comes in or only for the people who would deal with these codes?

Mr. Peter Davis: We do this for everyone who comes in.

Mr. Darren Fisher: Tell me a little bit about your recruiting process, when you're going out to search for new folks, and your training process.

Mr. Peter Davis: Sure.

Mr. Darren Fisher: Could you tell us a little bit about how you would train these folks up to be in a position where they understand the importance of being in possession of this taxpayer information?

Mr. Peter Davis: I'd be happy to.

Each year, we have what's called H&R Block Canada's tax academy. Starting in late summer, we begin taking applications from interested Canadians who want to take our training and become tax associates with us. Through that process, we teach them all about the tax code and how to work with Canadians in preparing and filing their taxes. We also spend time talking about security measures and how to ensure that taxpayer data is being treated with the utmost confidentiality at all times. This also includes information that is required in order to electronically file returns to CRA. There is quite a bit of training on that end.

For those individuals whom we choose to hire from our tax academy, we also provide additional training before they start with us preparing and filing taxes in our offices.

There is quite a bit of security and privacy training. That's held annually for all our staff every year.

Mr. Darren Fisher: I assume that it would be the norm within the industry for third parties and private sector organizations.

Mr. Peter Davis: I can't speak for all organizations, but it's certainly a norm for H&R Block Canada.

Mr. Darren Fisher: Okay.

When H&R Block Canada transmits a tax return to the CRA on behalf of the Canadian taxpayer through e-file, how do you ensure, from your end, that the data is secure?

Mr. Peter Davis: That information is transmitted through tax software, which is certified by the Canada Revenue Agency. Every tax software developer, including H&R Block Canada, has to undergo a rigorous certification process with CRA every year to ensure our tax software meets a number of CRA requirements.

In addition to that, we also have to make sure that tax software complies with all data privacy and data security legislation. There's a very comprehensive process that goes into ensuring that tax software is safe and secure for Canadians to use.

● (1615)

Mr. Darren Fisher: Have you had any breaches of any kind at H&R Block Canada of your clients' data?

Mr. Peter Davis: I'm unable to talk about any specifics around privacy breaches due to our data security and privacy policies. What I can say is that—

Mr. Matthew Green (Hamilton Centre, NDP): I have a point of order, Mr. Chair.

The Chair: Go ahead on your point of order.

Mr. Matthew Green: Mr. Chair, perhaps Mr. Davis isn't familiar with parliamentary proceedings or the powers of committees to demand testimony.

He doesn't have the ability, unfortunately, to sit behind some kind of pseudo client-solicitor privilege. He's here before Parliament, and he has to answer parliamentary questions.

I would ask that you apprise him of what his responsibilities are before the committee.

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

Mr. Davis, I understand the sensitive nature of the security system and the mechanisms that are in place within H&R Block. You made that very clear in your opening statement.

I would ask that you do answer the questions to the best of your ability. We are covered by parliamentary privilege, but we certainly don't want to put at risk—and I would agree with you on this—any proprietary issues within H&R Block that could cause problems. I'm going to direct you in that way.

Mr. Green, I hope you understand that when the request was made to have H&R Block come before the committee, there wasn't a specific individual who was asked to come. H&R Block has sent Mr. Davis as a representative, and I am satisfied that he's answering the questions to the best of his ability given the nature of what we're dealing with.

I stopped your time, Mr. Fisher, when the point of order was issued, so you have a minute left.

Mr. Darren Fisher: Okay.

You may have already said this, but can you confirm that all of H&R Block Canada's client data is stored solely on servers that are 100% in Canada?

Mr. Peter Davis: In terms of how that information is stored—this is all disclosed to our clients, and we do attain their consent—there are instances where client data may be sent to the United States to our parent company, H&R Block. Those instances would include that being required in order to provide the client with a specific product or service. In some cases, it may be to notify them if there may be some products and services that they wish to avail themselves of. That data is largely stored there, and it is not included in any pixels or anything else that could be provided to other parties.

The Chair: Okay.

Thank you, Mr. Fisher.

Mr. Darren Fisher: Thank you.

The Chair: Mr. Villemure is next.

Mr. Davis, can you put your earpiece in, please, and make sure it's on English interpretation? Please make sure the volume is up so that you can hear it.

[*Translation*]

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

Mr. René Villemure (Trois-Rivières, BQ): Thank you very much, Mr. Davis, for being with us today.

I won't repeat my colleagues' questions, which were all relevant. I would rather talk about privacy. Could you describe H&R Block's privacy policy?

[*English*]

Mr. Peter Davis: Can I ask that the question be repeated? The last part cut out a little bit there.

[*Translation*]

Mr. René Villemure: Could you walk us through H&R Block's privacy policy?

[*English*]

Mr. Peter Davis: We have a number of client privacy policies in place at H&R Block Canada. The one that I'd like to highlight for the committee is what we call our privacy assurance form. This is what we consider to be a gold standard within the industry here in Canada. We take the time to sit down with our clients in our offices, and we explain to them how their data is being used by H&R Block Canada and why. We take great consideration in limiting the use of the data to just ensure that it's used for what the client needs in order to have the products and services they expect. We sit down and talk through how this data is used. We talk about a number of provisions related to it, and we seek the client's consent in order to proceed as we've laid out.

What makes our privacy assurance policy a little unique is that, each year, when our clients come back to see us in the following tax seasons, we will also walk through any changes to that privacy assurance form. It's very important to us that our clients understand the importance we place on protecting their data. We want them to be informed and comfortable with the processes we have in place to protect their personal information.

● (1620)

[*Translation*]

Mr. René Villemure: You are probably familiar with the European Union's General Data Protection Regulation, or GDPR. Is the H&R Block gold standard in line with the GDPR or just the current Canadian protection?

[*English*]

Mr. Peter Davis: It is certainly required by Canadian legislation. I don't know offhand for sure if it's also compliant with the GDPR. I will follow up in writing once I get some confirmation on that.

[*Translation*]

Mr. René Villemure: That's perfect. Thank you very much.

You were just talking about consent. Do you believe that clients of H&R Block understand what they're actually consenting to?

[*English*]

Mr. Peter Davis: We take great pains at H&R Block Canada to make sure that our clients really understand how we use their information in order to provide them the products and services they expect. Our tax professionals across Canada are trained to really invest the time and sit down to explain our privacy protections and data policies in plain language. I can say with a high level of confidence that our clients do have a good understanding of how their data is used.

[*Translation*]

Mr. René Villemure: Consent forms are often one page long and written in legalese. That's why I'm going to ask my next question.

How long after tax filing do you keep your clients' data?

[*English*]

Mr. Peter Davis: We will keep their information as per statutory requirements, which I believe is the tax year and six years in addition to that, so seven years. I'm not aware of any other retention that we do beyond that, but I will confirm that and follow up with the committee in writing.

[*Translation*]

Mr. René Villemure: At the end of the retention period, how do you keep data on tax returns?

[*English*]

Mr. Peter Davis: We undergo a very comprehensive process to ensure that all personal information, once it's no longer required to be retained, is completely destroyed. It's very comprehensive.

[*Translation*]

Mr. René Villemure: Can you tell us in concrete terms how you do that?

[*English*]

Mr. Peter Davis: I probably cannot provide much more information on that, given our data security and privacy policy, I'm afraid. I will check with our office to see if there are any more details that we may be able to provide, and I will follow up in writing on that.

[*Translation*]

Mr. René Villemure: Okay.

Thank you very much.

The Chair: Thank you, Mr. Villemure.

[*English*]

Just to be clear, Mr. Davis, the clerk has been noting the answers where you will be following up in writing. She's going to follow up with you to ensure that the information does come to the committee. That is a reasonable compromise that the committee can deal with when it comes to providing sensitive information in confidence to the committee, as well.

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

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

Mr. Davis, you referenced in your opening remarks that H&R Block has never sent any client's personal data, including pixels, to companies such as Google and Meta. You referenced, of course, that this is H&R Block Canada.

Can you describe, for the purpose of this committee, who actually owns the proprietary data H&R Block has—the Canadian subsidiary or the American parent company?

● (1625)

Mr. Peter Davis: When you say “proprietary data”, what do you mean, exactly?

Mr. Matthew Green: That's the personal information of your clients, sir. You mentioned that some of it goes down to the States. Could we not venture, as it is a subsidiary of H&R Block Incorporated, in Missouri, that all of the information would be owned by the parent company as well?

Mr. Peter Davis: We don't own the information Canadians provide us. That is between H&R Block Canada and our clients.

I want to be careful how I answer your question, though, because I don't know all the ins and outs regarding the legalities of who would ultimately be the holder of that information. If you don't—

Mr. Matthew Green: Mr. Davis, I have limited time. I'll take my time back.

You specifically referenced that H&R Block Canada has never sent clients' personal data, including pixels, to companies such as Google and Meta. Yet, in July 2023, a United States Senate investigation determined that H&R Block most likely disclosed consumers' return information to Meta in violation of sections 6713 and 7216 by embedding Meta's pixel within the H&R Block mobile and website tools that consumers can use to prepare their personal tax returns.

Sir, are you familiar with the current class action lawsuit being filed against H&R Block in the United States?

Mr. Peter Davis: We take the security of our clients' personal information—

Mr. Matthew Green: I just asked whether you're aware of it.

Mr. Peter Davis: I am aware of it, yes.

Mr. Matthew Green: Okay.

You're aware that the lawsuit comes under their RICO laws, or the Racketeer Influenced and Corrupt Organizations Act, against the tax preparation company—your parent company—and Meta. This is a practice that was established by your parent corporation. Yet, it's your testimony here, with assurance, that H&R Block Canada has never sent them any client's personal information.

Can you make that assurance on the record here today, in this committee, that the same can be said for your parent company in the States?

Mr. Peter Davis: I'm here in my capacity as a representative of H&R Block Canada to talk about our Canadian clients and taxpayers. I can say with certainty that their data is not shared with companies like Google and Meta.

Mr. Matthew Green: You mean, by H&R Block Canada.

Mr. Peter Davis: That's correct.

Mr. Matthew Green: That wasn't my question.

My question is, can you make that same assurance to us on behalf of your parent company, which is currently under investigation for the very same practices you're being accused of here in Canada?

Mr. Peter Davis: When it comes to the data of our Canadian clients, neither H&R Block Canada nor H&R Block is disclosing that data to companies like Google and Meta.

Mr. Matthew Green: That only happened in the United States of America.

Mr. Peter Davis: I can't speak to where it may have happened. I'm here in my capacity as a representative of H&R Block Canada.

What I can say with certainty is that our Canadian clients' data was not involved in any sharing whatsoever with companies like Google and Meta, whether through H&R Block Canada or H&R Block.

Mr. Matthew Green: However, you are familiar with a Senate hearing determining this in the United States.

Mr. Peter Davis: Yes.

Mr. Matthew Green: It's not a wild assertion that you would also be doing the same practices, given that you're the subsidiary of a parent company being accused of the same thing.

Mr. Peter Davis: We're not sharing any Canadians' data with companies like Google or Meta at H&R Block Canada or H&R Block.

Mr. Matthew Green: I have a consumer question. It's related to the FTC's action that stopped H&R Block's unfair downgrading practices and deceptive promises of free filing.

Do you also offer the same type of free filing here in Canada?

Mr. Peter Davis: I can't speak about the specific filing products and services of H&R Block.

I can speak a bit about what we offer here at H&R Block Canada.

Mr. Matthew Green: Sir, I'm going to ask you the question: Are you familiar with the FTC requiring your parent company to pay $7 million to consumers?

Mr. Peter Davis: I am familiar with the action by the FTC.

Mr. Matthew Green: I'm asking you whether the product that has just resulted in a settlement there is also offered here in Canada.

Mr. Peter Davis: No, it is not.

Mr. Matthew Green: Okay, that will suffice for my round of questions.

Thank you.

● (1630)

The Chair: Okay. Thank you, Mr. Green.

That concludes the first round. We'll now go to the second round.

Mr. Chambers is going to kick it off for five minutes.

Mr. Adam Chambers (Simcoe North, CPC): Thank you, Mr. Chair.

Mr. Davis, thank you for coming. I apologize for missing your earlier round. Someone played a funny trick on me this holiday season and sent the minister of the CRA at the same time to the finance committee, so that's where I was for the first few minutes.

Bring me back to the issue at hand here. Does H&R Block Canada have obligations under the federal Privacy Commissioner and the federal Privacy Act?

Mr. Peter Davis: Yes, with respect to the issue that the committee—

Mr. Adam Chambers: I mean just in general.

Mr. Peter Davis: Yes, we do.

Mr. Adam Chambers: Okay.

Under that act, if there is a data breach—since H&R Block would be governed under or subject to the provisions of that act—H&R Block would be required to report on that data breach, if it was known to them, to the Privacy Commissioner. There is a reporting regime.

Mr. Peter Davis: That is correct, yes.

Mr. Adam Chambers: To my knowledge, there has not been a report from H&R Block to the Privacy Commissioner with respect to any breaches, including the ones that were in the news recently. Is that correct?

Mr. Peter Davis: Given that our investigation, once we were informed by CRA of the incident involving our e-file credentials.... We commenced our investigation immediately after learning about it. We went through a comprehensive investigative process, and its conclusion pointed to no evidence of any breach of our systems, software or security apparatuses at H&R Block Canada. As a result, there was no requirement or basis for us to report anything to the Privacy Commissioner.

Mr. Adam Chambers: I assume that, with your parent company, you not only invest a lot of resources in terms of treasure into cybersecurity and privacy breaches, but also share information about potential schemes or frauds that are perpetrated on various tax authorities, say, in Canada and the U.S. You're aware of some of the things that happen and how people's accounts get hacked. Is that correct?

Mr. Peter Davis: We are aware from what we see in the media sources that we monitor. In a lot of cases, it's not typical for the CRA to share that type of information with industry as of yet. Of course, there's also some information sharing between H&R Block and H&R Block Canada Inc. when it comes to cybersecurity.

Mr. Adam Chambers: In effect, I think I'm getting from your testimony that protecting privacy and people's personal information—their tax information but, more importantly, their private, personal information—is a core principle of what guides you as an organization. You have a lot on the line in order to protect people's personal information and their privacy in general.

Mr. Peter Davis: Absolutely. We've been doing taxes in Canada for our clients for over 60 years. Data protection and the privacy of our clients' information are absolutely paramount to what we do.

Mr. Adam Chambers: I won't ask you to answer this, because it would potentially be unfair, but I'll say this. It is your business to keep people's information private and secure. There have been a number of other examples of outright fraud perpetrated on CRA, with a number of examples of fraud happening on the taxpayer, fraudulent schemes, and things that are not audited correctly at CRA. The absence of your reporting anything to the Privacy Commissioner tells me that this issue is likely not one that is emanating from within H&R Block, but it could be an outside source, whether that's a third party or maybe even within CRA. I'm not sure.

I won't ask you to comment, because I think that might put you in a difficult position, but when you have CRA saying "It's not us" and you have a list of examples in the past where they've had some challenges with fraud and protecting private information, that makes sense to me. I think your testimony is genuine, and I hope that, to the extent that you find any information, you will bring it forward.

Can you follow up? You mentioned the CRA not collaborating as much with industry, but that does happen in the U.S. Is that correct?

● (1635)

Mr. Peter Davis: My understanding is that there are mechanisms for collaboration between the IRS and the tax preparation industry in the United States—namely, the security summit. We don't have a similar mechanism here in Canada, and that is something that would be beneficial for CRA to consider.

Mr. Adam Chambers: Thank you for that testimony, Mr. Davis, and congratulations on 60 years in business.

Mr. Peter Davis: Thank you.

The Chair: Thank you, Mr. Davis.

Thank you, Mr. Chambers.

Mrs. Shanahan, go ahead, please, for five minutes.

Mrs. Brenda Shanahan (Châteauguay—Lacolle, Lib.): Thank you, Chair.

I want to touch on a few things. I want to make the distinction between why we're here now, which has to do with *The Fifth Estate* report that it was through fraudulent use of H&R Block's special credentials for accessing the CRA website, something that's been built up with private companies and the CRA over the last couple of decades for the use of online filing.... Somehow, somebody got those credentials and used them to change information and pose as imposters to access the CRA website. The other bucket has to do with the sharing of clients' private information.

On the first thing, I find curious your lack of curiosity about how that came to be, your lack of co-operation and your company's lack of co-operation. Historically, I think there has been tremendous co-operation between private tax preparation companies and the CRA to make sure that this wouldn't happen.

Mr. Peter Davis: I wouldn't say there hasn't been co-operation. We have certainly been in communication with CRA throughout this incident, to the extent possible, and we have—

Mrs. Brenda Shanahan: Mr. Davis, what would make the CRA say that it was H&R Block?

Mr. Peter Davis: I'm sorry. What would make the CRA say that it was H&R Block for...?

Mrs. Brenda Shanahan: The report we have alleges that hackers had obtained confidential data used by H&R Block. It had to do with the confidential credentials that H&R Block uses to access the CRA. Someone, somehow, in H&R Block.... It could be an employee. It could be someone who had access, or it could be a third party, as Mr. Chambers alluded to. I want to get to that in just a moment.

Mr. Peter Davis: To be clear, as I mentioned earlier, we take the protection of our clients' personal information with the utmost seriousness. I just want to reiterate—

Mrs. Brenda Shanahan: It's not the personal information. Somehow, somebody got a hold of your codes.

Mr. Peter Davis: Yes.

Mrs. Brenda Shanahan: Why would the CRA say that it was the H&R Block codes that were used?

Mr. Peter Davis: I was just going to get to that.

Our investigation did not suggest in any way, shape or form that our systems were compromised or our security apparatuses or software—

Mrs. Brenda Shanahan: Your contention is that your codes were not used in this breach. Is that your contention?

Mr. Peter Davis: No, my contention is that H&R Block Canada and our software systems and security apparatuses were not compromised, so we were not responsible for—

Mrs. Brenda Shanahan: You go back to that, but somebody could have still used your codes and left them untouched so that you would not know that they, in fact, had been used. It was CRA on the other side that said, “Hmm, these codes are being used.”

Mr. Peter Davis: Yes, and we've never heard from CRA in any way, shape or form that they believe this information was compromised by H&R Block Canada.

Mrs. Brenda Shanahan: We'll put that aside, but I really do think it's important that there be co-operation among all parties in this regard, now and in the future.

Around the disclosure of personal information, you do say the following on your website:

> We do not disclose your personal information to third parties except as described in this Privacy Policy, with your consent, or as permitted or required by law. Your personal information may be disclosed....

I take Mr. Villemure's point that people do not always know what they are consenting to, but here's what they're consenting to:

> To outside suppliers employed or retained by us or by H&R Block US to perform certain services or functions...including...processing of...transactions, marketing, Instant Refund® processing....

That's there for others who want to read it. I have a second copy if people want to read it.

Also, the website states that this information would be “used or stored in the United States and will, in addition to Canadian laws, also be subject to the laws of the United States.”

I think that's something many Canadians would not know, that their information is being stored in the United States, which can be an issue for some people.

● (1640)

The Chair: We're past your time, Mrs. Shanahan.

Mr. Davis, I'm going to give you a chance to respond quickly. Go ahead.

Mr. Peter Davis: I'd just like to point out, as I mentioned earlier, that we take great pride in the client privacy framework that we have in our retail offices at H&R Block Canada. A big part of that is walking with our clients through our privacy assurance form process: exactly how their information is being used in order to provide the products and services they expect. The items you were referring to are items that we do walk through with our clients. We make sure they understand what that means, and we make sure to get their consent.

The Chair: Thank you, Mr. Davis.

[*Translation*]

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

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

Mr. Davis, have there ever been customer data breaches in the past at H&R Block?

[*English*]

Mr. Peter Davis: I'm not able, due to our data security and privacy policy, to discuss any sort of details about that particular subject matter, but what I can tell the committee—

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

The Chair: Go ahead, Mr. Green, on your point of order.

Mr. Matthew Green: Mr. Chair, I don't think Mr. Davis quite understands what process he's in right now. This is not like a textbook response that he can provide Parliament and not actually have to answer basic questions.

If he's not comfortable answering these questions at committee, I would, through you, Mr. Chair, request that he provide that to our committee in writing—if he does not want to do it on the record right now in front of the audience—for the consideration of this committee. We could then determine the worthiness of reporting on it. He can't simply come here to committee, a parliamentary committee of the House of Commons, and refuse to answer basic questions.

The Chair: Just let me deal with this, Mr. Davis.

Mr. Green, I fully agree with your assessment that these answers can be provided in writing to the committee, if it is the desire of the committee to do so. If that's what you want to do, Mr. Green, if we want information to be provided to the committee, we can certainly do that.

I believe that Mr. Davis is sincere in his attempts to answer the committee's questions. Again, as I said earlier, I understand that there's also some sensitive nature here. If the nature of any questions is sensitive enough, then we can request a written response from Mr. Davis on these issues, for the sake and benefit of the committee.

Mr. Barrett, on that point of order, go ahead, sir.

[*Translation*]

Mr. Villemure, I stopped the clock.

[*English*]

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): It has happened a couple of times. I fully agree with Mr. Green's intervention. Obviously, the witness is required to provide a fulsome answer, to the best of their ability, to any of the questions that are put forward by members of the committee.

As you said, Chair, it's up to the committee if we're willing to accept an answer in writing. That's the proposal from Mr. Green. I don't have any objection to that. It should be noted, though, that it remains the committee's prerogative whether that information is held in confidence, or whether we publish that information—if it's perhaps, simply put, in the public interest—but certainly there is no discretion on the part of the witness to answer or not to answer the question.

While we don't have an objection to the response to this question from Mr. Villemure being provided in writing, an answer must be provided.

The Chair: Based on the two points of order, I think it's pretty clear where the committee stands on this, Mr. Davis.

I don't want to speak for other members of the committee, but if it's your contention that this information can be provided to the committee, then I would recommend that you do that, and the committee will dispose of it in whatever fashion it determines, based on how it affects this study for us as well, because this is a very serious issue for Canadians. I hope you understand that.

There is another option for the committee, too. That is to go in camera and deal with this, but I don't really want to entertain that unless it's the will of the committee to do that.

Mr. Green, are you okay with that?

● (1645)

Mr. Matthew Green: Yes. Just on the point of order—and this isn't about Mr. Davis in particular, as I know he's here in his capacity—I just want the committee to note that this is a long-standing trend that we're now seeing when corporations send their public relations or government relations people and not the president. Moving forward, I think what we need to do with this committee, in order to get fulsome answers, is to actually have people here who have the power and the discretion to speak on behalf of the corporation that we're speaking to.

I would ask that you take that into consideration for future invitations.

The Chair: Yes, I think we're going to have to be more specific when we propose motions about whom we want to come to the committee, to your point, Mr. Green. Is that correct? Okay.

[*Translation*]

Mr. Villemure, you have—

[*English*]

Mr. Peter Davis: Mr. Chair, can I please continue on the earlier point of order that was mentioned? I want to clarify very quickly that if there ever were a situation of a breach of information occurring, our company would be statutorily obligated to report—

The Chair: Hold on.

[*Translation*]

There's no interpretation.

Mr. René Villemure: The sound is going in and out. Sometimes there's interpretation, sometimes there isn't.

The Chair: Is it working now? Maybe it's the headphones that are faulty.

[*English*]

Is it not working at all?

I'm sorry, Mr. Davis. We're going to make sure that Mr. Villemure hears your point.

It's not really on the point of order. I've given you a little latitude on this one, Mr. Davis, just because we have less time than normal.

[*Translation*]

It's working now, Mr. Villemure.

[*English*]

Mr. Davis, perhaps you can quickly state the point you want to make.

Mr. Peter Davis: Thank you.

Very quickly, if there ever were a situation of information being part of any type of breach, our organization would be statutorily obligated to report that information to the Privacy Commissioner.

We're not trying to be evasive here in front of the committee, but we have to also respect our privacy policies.

The Chair: Thank you. That's wonderful.

[*Translation*]

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

Mr. René Villemure: Thank you very much.

All of those question marks were part of my question as well. Thank you.

I wasn't asking you what steps had been taken. I was asking you whether or not there had been such leaks.

[*English*]

Mr. Peter Davis: Thank you for the question. Are you referring to the incident with the e-file credentials, specifically? Okay.

Our investigation absolutely addressed that piece as well, and there has never been an incident involving our e-file credentials in the past.

[*Translation*]

Mr. René Villemure: Okay.

I know you touched on this briefly earlier, but have all privacy breaches been reported to the Privacy Commissioner of Canada?

[*English*]

Mr. Peter Davis: I'm not an expert on the reporting of privacy breaches, but what I can say is that if there was a situation that required us to report something to the Privacy Commissioner, that would absolutely take place.

[*Translation*]

Mr. René Villemure: Would it be possible to ask your team to provide us with that answer?

[*English*]

Mr. Peter Davis: Yes, I can. Thank you.

[*Translation*]

Mr. René Villemure: That's great.

Thank you very much, Mr. Chair.

The Chair: Thank you, Mr. Villemure.

[*English*]

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

Mr. Matthew Green: Thank you very much.

I would like to go back to the opening statements on the idea of private sector breaches in security.

During his appearance on December 5, 2024, the Privacy Commission of Canada stated, “Data breaches represent one of the most significant threats to personal information globally. In the 2023-2024 fiscal year ending on March 31, 2024, my Office received over 350 reports of cyber incidents, the vast majority, or over 90%, from private-sector organizations.”

Mr. Davis, in your opinion, do these statistics show that cyber-incidents are more frequent and more likely to occur in private sector organizations than in federal government institutions?

● (1650)

Mr. Peter Davis: I'm not a privacy breach expert, so I'm not able to offer an opinion on where breaches like these would tend to take place more often than not.

Mr. Matthew Green: Mr. Davis, you came to provide expert testimony.

In your letter to the committee, you said, “There is no credible basis to support the notion that CRA automated tax filing and prefilled tax returns will further secure taxpayer information.”

Based on the very general statistic I just provided you, how do you explain the difference between government breaches and private sector breaches?

Mr. Peter Davis: I'm sorry, but I don't see the connection between CRA automatic tax filing and potential breaches of information by the private sector. Can you clarify that for me a little?

Mr. Matthew Green: Yes, I'm happy to.

Out of all the incidents, 90% of the privacy breach reports were from private sector organizations and 10% were from the government. Would that logic not extend to private sector organizations being more vulnerable to privacy breaches?

Mr. Peter Davis: As I stated earlier, I can't provide an opinion on statistics that I'm hearing just second-hand now. I'm unable to make an informed judgment on that.

Mr. Matthew Green: What do you think explains the difference?

Mr. Peter Davis: Again, I can't speak or give an informed opinion on statistics that I'm hearing second-hand just now.

Mr. Matthew Green: Okay.

Mr. Chair, through you to Mr. Davis, can he please provide to the committee, in writing, a policy in the event of a breach of client data? Basically, what I'm requesting is H&R Block Canada's policy in the event of a breach of information for client data.

The Chair: Okay. Thank you, Mr. Green. The clerk has made a note of that. We'll follow up with Mr. Davis and make sure that that information is supplied.

Mr. Barrett, go ahead for five minutes.

Mr. Michael Barrett: Mr. Chair, on December 6, I gave notice of a motion that I'm going to move now:

> That the committee undertake a review of the data privacy and contracting policies employed by Export Development Canada (EDC) during the implementation of the Canada Emergency Business Account (CEBA) program, that the committee report its findings and recommendations to the House, and that the committee invite the following witnesses to testify:
>
> (a) Accenture CEO Julie Sweet and officials;
>
> (b) EDC CEO Mairead Lavery and officials; and
>
> (c) Auditor General of Canada Karen Hogan

The Chair: Thank you, Mr. Barrett. The motion is in order.

Do you want to speak to it?

Mr. Michael Barrett: Yes, I do.

The Chair: Okay.

Mr. Davis, I am going to ask you to leave, if you want. I would expect that, with the transition to the next panel and some discussion on this, this will conclude your testimony before the committee.

As I said earlier, the clerk has made note of the request of the committee. She'll share that with you, and the expectation of the committee is that you'll send that back to us in a reasonable time frame. The clerk will provide a date by which to provide that information, and it won't be Christmas Day. I guarantee that.

Thank you, Mr. Davis, for your testimony.

I'm going to go to Mr. Barrett now.

Mrs. Brenda Shanahan: I have a point of order.

The Chair: Go ahead.

Mrs. Brenda Shanahan: Mr. Chair, can we have the text of the motion? Usually, you give us some indication of what's coming.

The Chair: Okay.

Madam Clerk, was that motion sent to committee members previously?

The Clerk of the Committee (Ms. Nancy Vohl): Yes.

The Chair: Okay.

We'll send it out, Mrs. Shanahan, but I'm going to go to Mr. Barrett to keep things going here.

Go ahead, Mr. Barrett.

Mr. Michael Barrett: Mr. Chair, on December 2, the Auditor General issued a report, which is the basis for this motion. This was "Report 8: Canada Emergency Business Account" with respect to the COVID-19 pandemic. It's an independent auditor's report. On December 2, there was widespread media coverage on this very issue. Then, a notice of motion was given and distributed in both official languages to all members of the committee on December 6, so they've had ample time to become well apprised of both the motion and the situation in the official language of their choice. The Auditor General's reports, of course, are available in both English and French in their complete form online and were available in printed format, in advance of being tabled in the House, in an embargoed form, for all members.

To the issue, Canada's Auditor General found that Export Development Canada gave $314 million in sole-source contracts to administer loans. The government selected EDC to administer this emergency loan program. Then EDC turned around and said, "We don't have the capacity to do that, so we're going to outsource it." They outsourced hundreds of millions of taxpayer dollars in contracts.

Some of the details of these contracts are incredibly concerning. They were paying 14 hours per day to Accenture for their call centre work, but the call centre is open for only nine hours a day. The hourly per-person rate ranged between $60 and $750. Equally concerning is that Accenture outsourced some of the work to a Brazilian subsidiary. Therefore, these folks were receiving rates of $750 per person per hour to administer a program EDC was supposed to be delivering. "Generous" is an understatement. I'm quite certain there are no members of the public service who, in their capacity as public servants, are being paid $750 per hour. We have a massive conflict of interest here.

In concluding my brief remarks, I'll offer a quote from Karen Hogan, who is the Auditor General. She said, "not managing that conflict of interest, in my mind, was unacceptable". I couldn't agree more with the Auditor General. Of course, we're dealing with Canadians' personal information, Government of Canada programs and the type of conflict of interest that gives rise to a great concern. That conflict of interest was deemed "unacceptable" by the Auditor General.

Of course, that fits within the mandate of this committee. It's important. I don't think the study would take many meetings. The mandate of this committee is dealing with those conflicts of interest. While other committees can do what other committees do, this committee should do what only it can do. That's why I have put this motion forward today.

● (1655)

The Chair: Thank you, Mr. Barrett.

I saw Mr. Drouin first. I'll go to Mrs. Shanahan after that.

Mr. Matthew Green: Are you looking at the screen?

The Chair: I'm sorry, Mr. Green. I was wondering whether your hand was up. The backdrop is contrasted against something red that makes it difficult to see.

I'm going to Mr. Green first, because I was wondering whether he had his hand up. I couldn't tell, but he did.

Go ahead.

Mr. Matthew Green: Thank you very much.

It's just a simple question on the motion.

There is no timeline for this. I want to make it abundantly clear to this committee that I do not intend to be called back on some kind of surreptitious prerogative of the chair or Standing Order 106(4). This is an important issue; I agree. I think it is one that deserves our full attention when we return once the House is sitting. I want to be very clear about that.

Mr. Chair, can I ask whether that is the intention of this motion, or whether this is something they're looking to revive in the early weeks of January because there's a slow media cycle or something like that?

The Chair: Are you asking a question on that, Mr. Green?

Mr. Matthew Green: It's an honest question, through you, to the mover of the motion, because they did not provide a date or say, "when we return to the regular sitting of the House". Right now, it's just open.

I wouldn't want to be in a situation where we're called back from our constituents and families.

The Chair: The other issue here is that it doesn't define the number of meetings, Mr. Green. I've made note of that as well.

Do you want to respond to that quickly, Mr. Barrett? Go ahead.

Mr. Michael Barrett: We would, of course, be comfortable with an understanding in place of an amendment—that the committee is operating with the understanding, or the chair is charged with the understanding, that this motion will be dealt with following the resumption of the House in the last week of January. If the motion passes, I think we can all share that understanding without it being explicit.

With respect to the number of meetings, I think it could be few.

● (1700)

The Chair: Yes. Based on the number of witnesses in there, it would probably be no more than two.

Mr. Michael Barrett: We would have no objection.

The Chair: Okay.

Unfortunately, I'll need an amendment for that, unless there's unanimous consent on the part of the committee to adopt that no more than two meetings will be granted on this. That way we have some clarity on it.

There is nothing in this motion that says how many meetings. I'm going to ask for clarity and say that no more than two meetings be deemed for this particular motion.

Mr. Francis Drouin (Glengarry—Prescott—Russell, Lib.): Mr. Chair, maybe we want to hear from everybody else before we entertain how many meetings we want to have.

The Chair: We can do that.

Mr. Francis Drouin: We're still not sure if we're good to go.

The Chair: For the sake of clarity, I will need somebody to tell me how many meetings they want on this. It was my suggestion to do that in advance of hearing from people, but I will leave it at that.

Go ahead, Mr. Drouin.

[*Translation*]

Mr. Francis Drouin: I commend the efforts of my dear colleague Mr. Barrett. At the Standing Committee on Public Accounts, we're conducting a study on the issue of the Canada emergency business account. He knows that because he appeared before this committee. In fact, we're trying to do a study on the public accounts. For a few days now, we've been trying to schedule it, but the Conservatives are filibustering to not even hear from the witnesses. We had the Auditor General before us yesterday, and we had other witnesses as well, but the Conservatives filibustered.

Before voting on this motion, I would invite Mr. Barrett to speak with Mr. Perkins and Mr. Genuis, as well as Mr. Cooper, who also sometimes sits on the Standing Committee on Public Accounts. I therefore invite Mr. Barrett to speak with his colleagues. I'm all for effective parliamentary committees. If the Standing Committee on Access to Information, Privacy and Ethics decides to conduct this study on the Canada emergency business account program, you can rest assured that I will not be in favour of wasting taxpayers' money by conducting the same study at the Standing Committee on Public Accounts.

I know it's Christmas and we're all in a hurry to pass motions and go home and say that we've accomplished things, but I invite my colleagues to have a discussion with their other parliamentary colleagues.

[*English*]

In that spirit, Mr. Chair, I want to make sure we're not doubling services or parliamentary accountability. I truly believe in it, but we had many reports tabled in the House by the Auditor General on December 2. We had one on seniors. We had one on Canada summer jobs. Let's make sure our parliamentary committees function in a way that is efficient and that gets to the bottom of the issues. Let's not get stuck like we did with SDTC, where the industry committee was doing the same study at the same time, with the same members asking the same questions at both committees, and with the same witnesses.

I enjoy this idea, and I'm not a regular member of the ethics committee, but we're getting into a doubling of services. I'm sure the Conservatives would agree that this is not an efficient use of taxpayers' dollars when the public accounts committee...unless they can convince their folks at public accounts to let ethics do this particular study and let public accounts focus on other reports of the Auditor General. That way, I will be satisfied in terms of the way it's functioning.

I'm sure the honourable members, as they want to form government, would already have had these conversations with their colleagues to ensure greater efficiency of taxpayer dollars and how they are spent. We, too, spend dollars, and it's important that we show taxpayers respect.

The Chair: Thank you, Mr. Drouin.

We're obligated to deal with the motion that's in front of us. The motion is in order. It deals with data privacy and the potential of.... Well, we don't know; we'll certainly find out, if the motion is adopted, by having these witnesses in.

I see it as separate and distinct from what other committees are dealing with right now. This is a data privacy motion. It's well within the mandate of this committee.

Go ahead, please, Mrs. Shanahan.

● (1705)

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

I'm sorry that I didn't have the motion handy. I have a folder here, as you can see, with all the motions that have been presented in this committee. I do try to keep track. It is not easy to do so. I suppose we can dispense with those ones for now or keep them for a later date. Maybe they'll be revived. I don't know if anyone has any way...because it's just getting heavier and heavier. That's not good for my back, I can tell you that.

I'm sorry. I am old school. I do like paper. It allows me to read, analyze, take notes and so on.

I listened with great interest to my colleague from the public accounts committee. I think there is something to be said here. This is a topic that has come up on many an occasion, even in this committee: that we shouldn't be duplicating work.

You know, by all accounts, there's only a limited time left on our mandate here to the 44th Parliament. We should make the best use of it. There are many issues that we need to be discussing. I'd like to have an update on reports, perhaps, that have been left unfinished and work that needs to be continued from other motions that apparently other members are interested in pursuing.

I appreciate the offer of limiting this study to two meetings, but how about zero meetings? Let's let the public accounts committee do its work.

Indeed, while talking about letting somebody do their work, it has often been my observation that this committee attempts to do the work of our independent commissioners of Parliament, namely the Conflict of Interest and Ethics Commissioner, not to mention other commissioners from time to time. However, it's chiefly the Conflict of Interest and Ethics Commissioner. We try to get ahead of where he is if there is an issue. I'm sure that members are very capable of alerting the commissioner if they feel there's a conflict of interest issue, as are any members of the public. Anyone who is concerned about this situation could make that known to the commissioner.

We have seen him, in some cases repeatedly on the same complaint—one, two, three, four times—come back with the same conclusion. It apparently was not sufficient for members at that time, but it is still consistent with the role of an independent agent, an officer of Parliament. They do their work, their investigation, and make a report. That is something I certainly would suggest.

As it stands, I cannot support this motion.

Thank you.

The Chair: Thank you, Mrs. Shanahan.

For the benefit of the committee, I will say that we do have the CSIS director and other officials from CSIS in the room to discuss TikTok in our next panel.

I am going to go to Mr. Fisher, because he's next on the list on the motion.

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

Out of respect to the witnesses who are here, I'll be quick.

This is being studied in another committee. I agree that it could be the purview of this committee. Two meetings already have happened at the public accounts committee. I've heard members of this committee state fairly emphatically that they don't support duplication, studying the same thing at two different committees. We'll see how they vote on this.

I'm not going to support this at the moment. That doesn't mean that I wouldn't support it down the road, maybe after the public accounts committee's study. At this point, I'd say that I'd vote against this today. Then we would get our witnesses in.

The Chair: Go ahead, Mr. Housefather. You have the floor on the motion.

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

I will also be brief.

First of all, I have to say that I disagree with my dear colleague, Mrs. Shanahan, a little bit. I do believe very strongly in the oversight by committees of the work of the Auditor General and everybody else. I believe that is the role of parliamentarians. I have no issue with that.

My issue is that I've looked at this report and at the summary of the report, and there's not one thing about privacy that's even included in the summary of the report. This is a report about financial controls and contracts, which is not the purview of the ethics committee. It is the purview of the public accounts committee or OGGO. I don't understand why this is being brought to the ethics committee. I've looked through the summary. Privacy is not even mentioned as one topic in the entire summary of the report. For me, that really is the issue.

It's already being looked at by the public accounts committee. If the focus is not privacy, then I really don't think it's the purview of the committee. Although I think it would be fascinating to look at the contracting policies employed by EDC, which are part of this motion, I just don't think it's the role of the ethics committee.

Thank you, Mr. Chair.

● (1710)

The Chair: Thank you, Mr. Housefather.

I have nobody else on my list, so I'm going to ask—and I suspect I know the answer—whether we have unanimous consent on this motion.

Mr. Michael Barrett: I'd like a recorded division.

The Chair: We'll have a recorded division on the motion.

Go ahead, Madam Clerk.

We have a tie vote, so I will vote yes.

(Motion agreed to: yeas 6; nays 5)

The Chair: I'm going to suspend for a couple of minutes until we get the next panel in line here.

● (1710)

_____(Pause)_____

● (1715)

The Chair: Welcome back, everyone.

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Thursday, November 21, 2024, the committee is resuming its study of the wind-up of TikTok Technology Canada, Inc.

I'd like to welcome our witnesses for the second hour today.

From the Canadian Security Intelligence Service, Daniel Rogers is here as director, with Paul Lynd, assistant deputy minister of intelligence collection.

I'm going to go to you, Mr. Rogers. You have up to five minutes to address the committee. Go ahead, sir.

Mr. Daniel Rogers (Director, Canadian Security Intelligence Service): Thank you, Mr. Chair.

[*Translation*]

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

I have a couple of points, and I'll try to make them fairly quickly.

My name is Daniel Rogers, and I am the director of the Canadian Security Intelligence Service, or CSIS. I am joined by my colleague Paul Lynd, the assistant deputy minister responsible for intelligence collection.

It is an honour to join you today and to have the opportunity to contribute to your important discussion on the winding up of TikTok Canada. Today, I hope to provide insights on CSIS's role plays in ensuring the protection of Canada's national security interests, the safety of Canadians and Canada's prosperity.

The Investment Canada Act, or ICA, which is administered by Innovation, Science and Economic Development Canada, ensures that significant investments in Canada made by non-Canadians benefit Canada's economy. To this end, the act allows the government to review foreign investments to ensure they are not harmful to Canada's national security.

The act aims to strike a balance promoting economic prosperity and safeguarding Canada from foreign actors seeking to gain ownership or control of sensitive Canadian goods, technology, infrastructure or personal data for purposes that could be injurious to Canada's national security.

[*English*]

In accordance with its mandate, CSIS regularly screens ICA notifications for security concerns, and we work with ISED, Public Safety Canada and federal granting councils to inform the GC's decisions. This work is essential, as Canada is the target of a number of adversarial state actors looking to advance their own national interests at our expense through their investment activities.

Social media platforms in particular are of interest to threat actors because of the data they generate and collect. They run surveys, collate datasets and request access to users' personal data through terms and conditions, enabling access to photo albums, messages and contact lists, among other sensitive details. Although some of this data is benign in isolation, when collected and collated on scale, it can provide detailed patterns and insights on populations, public opinion, communities and individual social and professional networks.

Authoritarian states like the PRC use big data, including from the private sector, to carry out foreign interference activities. While government use of data in Canada is subject to ethical, legal and privacy considerations, authoritarian states are not subject to these limitations. Through its 2017 National Intelligence Law, the PRC compels PRC citizens and entities to co-operate with PRC intelligence agencies upon request, which includes providing all information to the state and its intelligence apparatus. This policy supports, and is reflective of, the PRC's attempts to interfere in Canada and like-minded democracies. Canada and its allies must therefore exercise heightened caution when agreeing to share their data with platforms linked to the PRC.

The ICA review process, which includes CSIS input, determined that allowing TikTok Canada to continue operating would cause injury to Canada's national security. Although the provisions of the ICA limit what I am able to disclose about specific cases, I would note that the CSIS and Government of Canada assessment was consistent with the March 2024 policy statement on foreign investment review in the interactive digital media sector. Specifically, assessments consider factors such as reach and audience, the nature and extent of an investor's ties to a foreign government, and whether a Canadian business is likely to be used as a vehicle by a foreign state to propagate disinformation or censor information in a manner inconsistent with Canadian rights and values.

● (1720)

[*Translation*]

Use of social media platforms also raises national security concerns when they act as a breeding ground for extremist ideologies and radicalize users. The increasing volume of violent rhetoric online raises our concern that consumers of this content are more likely to mobilize to violence. Youth in particular can be especially vulnerable to becoming radicalized online due to their more frequent use of social media.

CSIS continues to actively investigate, advise on, and disrupt national security threats. CSIS is also committed to building resilience through our modernized authorities under Bill C-70.

This new authority recognizes that protecting Canada's national security is a shared endeavour that includes partnering with all levels of government, Canadian communities, academia, the private sector, and others. We are committed to co-operating with these groups in the national interest, including through increased sharing of detailed threat information.

I will conclude by noting that while CSIS cannot publicly comment on our specific operational activities or investigations, I welcome this opportunity to answer your questions.

Thank you.

The Chair: Mr. Rogers, thank you for your presentation.

We will now begin the first round of questions.

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

[*English*]

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

Thank you, Mr. Rogers.

With respect to personal data being shared with the Beijing-based regime, you cited the 2017 National Intelligence Law. Theoretically, it would seem to be true that there is a risk that the data of Canadian users of TikTok will be shared with the PRC. However, the evidence we heard from TikTok, when they came before this committee a few weeks ago, was that data had not been shared and that, indeed, a firewall had been set up to prevent the sharing of such data.

Can you speak about that?

Mr. Daniel Rogers: I can speak to the first point, which is that there is a concern about the risk of that data going to the PRC. As I think this committee has heard before, that data is not housed entirely in Canada. There are questions about the applicability of Chinese law to Chinese companies, including the parent company of TikTok, which is ByteDance. It is certainly foreseeable that data held by TikTok Canada could, as you suggested, end up in the hands of the People's Republic of China.

Mr. Michael Cooper: At this point, it seems to me to be theoretical, and nothing more than that.

Mr. Daniel Rogers: I can't speak publicly to any specific instance of data that's gotten over there that we would have known about through intelligence, but that is a certain risk that many of us are concerned with from a national security standpoint.

Mr. Michael Cooper: From the standpoint that it is a risk, how does shutting down the subsidiary of TikTok affect that in any way? It would seem to me that it is entirely unrelated. To the degree that there is a risk, the risk continues, does it not?

● (1725)

Mr. Daniel Rogers: I think it's a fair point. You're correct that the subsidiary, TikTok Canada, does not eliminate the use of the application here in Canada, nor the data that it holds. I would note, going back to my opening remarks about the consistency of the decision with previous policy statements, that the decision-making in that context is in an ICA process. Certain events trigger decisions and reviews by the ICA, which is administered by ISED. CSIS provides national security advice in the context of those triggered reviews.

Mr. Michael Cooper: Thank you for that.

I will say that it is troubling to see the total lack of transparency on the part of this government with respect to this decision. The government, on one hand, is shutting down TikTok's subsidiary. At the same time, Canadians are free to use the app. I don't necessarily see why not, but there doesn't seem to be consistency. If the objective is concern, for example, about the use of personal information or about personal data being shared with the Chinese communist regime, the solution that the government has come up with doesn't seem to achieve that at all.

I would just try to at least understand, from the theoretical standpoint of personal data being shared with the PRC, that TikTok did set up Project Texas, which ensures that U.S. data stays in the United States.

I'm trying to understand. When you say that there is a risk and that some of that data could be shared and would not be housed entirely in Canada or would not remain in Canada, what do you mean by that? Could it be stored in the U.S., or what?

Mr. Daniel Rogers: The concern, in general, is that the parent company of TikTok Canada is a Chinese entity and subject to PRC laws, which could compel them to act in ways such as getting data or using the platform for other means that the Communist Party of China sees fit. That risk continues to exist.

Mr. Michael Cooper: Is it the case that the Chinese company, ByteDance, operates the algorithm and owns the algorithm?

Mr. Daniel Rogers: That's my understanding.

Mr. Michael Cooper: Okay.

In terms of that operation, is it in China, in the PRC, that the algorithm is operated?

Mr. Daniel Rogers: I'm not well placed to speak to the specific operations of TikTok. That would be a better question for them. I imagine that there is a more distributed nature of that. I couldn't speak to that with any credibility.

Mr. Michael Cooper: Okay.

In terms of risk, at least from a theoretical standpoint, it would certainly be an issue to the degree that the algorithm is operated by the Chinese company ByteDance. In order for the algorithm to work, data necessarily would have to be shared with ByteDance. To the degree that the algorithm is being handled by ByteDance in that regard, then yes, pursuant to the 2017 National Intelligence Law, they could be compelled to share data with the Beijing-based regime.

The problem is that I don't see any evidence that this, in fact, has actually happened. It seems to be entirely theoretical.

The Chair: Thank you, Mr. Cooper.

We're over time.

Mr. Rogers, do you have a quick response to that? It was more a comment than a question, I think.

Mr. Daniel Rogers: I think I've answered that. I'm happy to—

The Chair: Okay.

For the benefit of the committee, I did ask the clerk to reach out to TikTok to see if they would be available, because I thought they would be material to this discussion. As you may or may not know, they did file a legal challenge against the federal government shutdown order, so, not surprisingly, they weren't available to appear today.

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

● (1730)

Mr. Anthony Housefather: Thank you very much.

Director Rogers, welcome to the committee.

It's nice to see you, Mr. Lynd.

Mr. Cooper's questions were very good, but I don't think they related to the ICA decision. The ICA decision had nothing to do with Canadian users' privacy; it had to do with national security issues other than that. Otherwise, we would have banned the app completely, if we were dealing with the privacy issues.

Is that correct?

Mr. Daniel Rogers: I hope this answers your question.

Yes, you're right that the ICA decision was specific to TikTok Canada, because that's the transaction that triggered the review.

Mr. Anthony Housefather: Looking at that, in its legal challenge, TikTok Canada argued that there were procedurally unfair things that happened related to the national security review.

I presume you would disagree with that contention.

Mr. Daniel Rogers: It's actually important for me to say that CSIS forms one part of that review. Our context in that review is to provide national security advice and assessments, which go into a broader context of decision-making. Very appropriately, the overall decision is not made by CSIS; it's made by others. There are protections around that decision, which include cabinet confidence, national security confidentiality and information that might be proprietary to the company. There's a limit to what I can say specifically, also because there is a matter in front of the courts, which I can't comment on.

I can say that CSIS participated in the decision. We did provide national security advice related to the decision. As I mentioned in my opening remarks, the decision was consistent with the policy. That's about what I can say.

Mr. Anthony Housefather: I understand.

Without asking you if CSIS gave, in its own advice, the decision to do what the end decision was—which was to require the company to close—can I ask you if CSIS, in its review, found significant security concerns posed by TikTok operations in Canada related to foreign influence?

Mr. Daniel Rogers: I can say that CSIS did provide national security advice and that we did find that there were national security reasons to be concerned with TikTok Canada's establishment. The ultimate decision was what it was.

Mr. Anthony Housefather: Was one of the considerations what the American Congress decided to do, which was to say that within a certain amount of time, they would have to sell the company to a domestic or American owner?

Mr. Daniel Rogers: That's not an input that CSIS would have provided into this decision.

Mr. Anthony Housefather: You weren't looking at it through anything other than the framework of the law to say yes or no, whether there are concerns that would require you to then take action.

Mr. Daniel Rogers: That's correct. CSIS has a fairly prescribed role, which is to provide national security assessments to input into the decision-making process.

Mr. Anthony Housefather: Let me come back to the privacy questions that Mr. Cooper was asking.

The former CSIS director, David Vigneault, had warned Canadians that they should steer clear of the TikTok app because it poses a data security risk.

Would you concur with that advice? Is that also your advice?

Mr. Daniel Rogers: I think Mr. Vigneault made a reasonable statement there.

I have to stick with my role in CSIS, which is not to make decisions or recommendations on behalf of the government.

I can certainly be clear that there are national security risks that we would assess inherent to TikTok as a platform, relating to what I described earlier about the potential for data, algorithms and other things to be used by the PRC contrary to Canada's interests.

Mr. Anthony Housefather: While I have you here, is CSIS currently reviewing or has CSIS reviewed the algorithms of TikTok to determine if misinformation is being circulated on TikTok in different areas? For example, are TikTok's algorithms furthering anti-Semitism in Canada by teaching a narrative that turns people or users against the state of Israel?

Mr. Daniel Rogers: I will certainly say that rhetoric and narratives like the narratives that you describe are pervasive across many social media platforms, not just TikTok Canada. I don't have a specific point to raise here about TikTok Canada's algorithm specifically in relation to that.

As I mentioned earlier, we're very concerned with the amount of content online that serves to radicalize particularly youth against any number of targets, including the Jewish community, the LGBT community and many other targets. That's a trend that we're consistently and increasingly worried about.

Mr. Anthony Housefather: Would I be at least correct in assuming that this is ongoing activity that CSIS is looking at with respect to monitoring extremism coming through the TikTok platform and other similar platforms being used today in Canada?

Mr. Daniel Rogers: Yes, it's TikTok and other platforms. In fact, we and our Five Eyes allies, along with our law enforcement allies, recently put out a press release and guidance related to the radicalization of youth online very specifically. It's a challenge for us investigatively, because often people are radicalized only online, and particularly youth. That is a worrying trend.

● (1735)

Mr. Anthony Housefather: Thank you.

Do I have any time left, Mr. Chair?

The Chair: You have one minute and 10 seconds.

Mr. Anthony Housefather: Okay.

I'm sorry. You're still stuck with me.

I'll go back to the algorithm you mentioned. To my understanding, TikTok Canada's algorithm would be no different from the algorithm being used by TikTok in the United States and in other countries, at least according to what I've heard from TikTok. One of the issues related to what I understand has happened in TikTok is that considerable misinformation has been floated for the U.S. elections in 2016, 2020 and possibly 2024 through the TikTok platform.

Has CSIS looked at what we would need to do to protect ourselves in the Canadian election that we expect to have next year, in 2025?

Mr. Daniel Rogers: CSIS has been very preoccupied with the concerns around foreign interference in elections, as I'm sure you're aware. That includes the possibility for threat actors to use social media platforms to advance disinformation or other narratives harmful to Canada's interests. I would say that's not a platform-specific concern that we have. That's more around the intent and plans of foreign adversaries to use platforms, however they might get their—

Mr. Anthony Housefather: I'm talking specifically about the Government of China, a foreign adversary—we have a special parliamentary committee dealing with China—using their algorithm on TikTok, which we understand could be controlled by the Chinese government, or certainly Chinese sources, to try to help one side or another in a Canadian election.

The Chair: You know you're over time.

I will need a very quick response.

Mr. Anthony Housefather: I'm sorry.

Yes. It can be very succinct.

The Chair: I'll let you give a quick response, Mr. Rogers.

Mr. Daniel Rogers: My succinct response is that this is one of the concerns we worry about, based on the PRC's law and the use of TikTok.

Mr. Anthony Housefather: Thank you.

The Chair: Thank you, Mr. Housefather.

[*Translation*]

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

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

Thank you for being here today. I think your remarks are clear.

There was a reference to a comprehensive review. What is a comprehensive review?

Mr. Daniel Rogers: What is a review?

[*English*]

For us, I think it depends. In the context of an investigation, this might be an investigation into a particular threat actor. In the context of TikTok and the ICA, this would be a review of the activities of a particular company, its ties to foreign governments and any particular data that CSIS might have in its intelligence holdings that might inform the potential for a foreign actor to make use of a transaction contrary to Canada's interests.

[*Translation*]

Mr. René Villemure: Could we talk a bit more about the national security risks that led to the liquidation of TikTok?

Mr. Daniel Rogers: Yes, a little bit, but as I said earlier, I can't give specific details.

[*English*]

I will say that in this case, as mentioned, there are concerns about the use of TikTok as a platform more generally. TikTok Canada is obviously affiliated with that platform. Those two things are not unrelated.

I can't speak to the specific concerns we would have with respect to TikTok Canada, given the issues I raised earlier.

[*Translation*]

Mr. René Villemure: The reason for my question is simple. In the past, national security has sometimes been interpreted very broadly and used as a pretext.

Can you tell us about ByteDance and its shareholder? It owns TikTok, as we know, but does it also have other activities?

Mr. Daniel Rogers: Are you talking about ByteDance's activities in general?

Mr. René Villemure: Yes, and I'm also talking about its shareholder.

Mr. Daniel Rogers: Okay.

[*English*]

In general, ByteDance is a Chinese company. That is the main preoccupation for us in the context of this review. It certainly operates the TikTok application, which is a global application that hosts many, many millions of users. It is subject to the PRC national security regulations. It has the potential to be used by China contrary to Canada's interests.

[*Translation*]

I'm sorry, I don't know if that answers your question.

Mr. René Villemure: Who owns ByteDance?

Mr. Daniel Rogers: I don't know exactly.

Mr. René Villemure: We often hear about the fact that ByteDance's board of directors is made up of French people, among others, but I believe that the founder of TikTok is still very present in the shareholding.

Mr. Daniel Rogers: I don't know. I wouldn't want to give inaccurate information.

Mr. René Villemure: Apart from sharing information with the Chinese Communist Party, are there other forms of collaboration between TikTok, ByteDance and the Chinese government?

● (1740)

Mr. Daniel Rogers: As Mr. Cooper said, there are some theoretical concerns there. We know that China's national security law applies to ByteDance and the operations of TikTok.

[*English*]

I can't speak to specific intelligence we have that links to anything concrete that we know through intelligence channels.

[*Translation*]

Mr. René Villemure: In your investigation on behalf of the department, did you collaborate with the Privacy Commissioner of Canada?

[*English*]

Mr. Daniel Rogers: We speak with the Privacy Commissioner regularly. In the context of these reviews, typically the assessment is done by CSIS based on its intelligence knowledge and threat assessments.

[*Translation*]

Mr. René Villemure: Does this type of review take place more often than others, for example?

Mr. Daniel Rogers: Yes, I think CSIS did over 1,000 last year.

Mr. René Villemure: Okay, that's a lot.

Is the final report now available?

Mr. Daniel Rogers: Our advice to the government?

Mr. René Villemure: Yes.

Mr. Daniel Rogers: No, it's not publicly available.

[*English*]

It's part of our advice to government. It is often subject to other provisions, like cabinet confidence, in the decision-making process, and as I mentioned earlier, it will contain classified information and sometime private information from the company.

[*Translation*]

Mr. René Villemure: My concern is similar to Mr. Cooper's. We're being told both that we need to ban TikTok and that we can continue to use it, that's our choice. I find it ironic.

Were you involved in the Government of Canada's decision to ban TikTok from government devices?

[*English*]

Mr. Daniel Rogers: Banning TikTok on government devices was a decision made by the Treasury Board of Canada. From our point of view, data collection by TikTok, particularly from government devices, could cause national security concerns, and I think those are on some level different from the general use of TikTok.

I should say that the decision-making process for many of these decisions, not just with the Investment Canada Act but in the Government of Canada's decision to ban TikTok on government devices, takes into account many different factors, not just national security. They can include economic factors, social factors and others. When it comes to government decisions, we think about government data particularly and the national security concerns that would be inherent in the data.

[*Translation*]

Mr. René Villemure: Do you use TikTok?

Mr. Daniel Rogers: No.

Mr. René Villemure: Mr. Lynd, do you use TikTok?

Mr. Paul Lynd (Assistant Deputy Minister, Intelligence Collection, Canadian Security Intelligence Service): No.

Mr. René Villemure: Okay.

Thank you, Mr. Chair.

The Chair: I don't use TikTok either. I don't see the point of it.

[*English*]

Mr. Green, go ahead for six minutes. Do you use TikTok?

Mr. Matthew Green: Yes, I did quite regularly, but stopped once the Canada-China investigations revealed the targeting of MPs. Certainly, the instances of social media interference or influence within democratic political election processes are well noted and well documented. To go back to 2016, you'll recall Cambridge Analytica, and there are lots of instances with Elon Musk's participation in the most recent election in the States.

Mr. Rogers, first of all, well welcome to committee. I think this might be the first time I've had a chance to chat with you. In your opinion, how does TikTok differ materially from other social media platforms in the way user information, data, algorithms and profiles are used?

Mr. Daniel Rogers: To the extent that I can answer the question, I will say there are general concerns that Canadians and others have about the social media platforms we're engaged in. These are things like the spread of disinformation and the ability for platforms to be used by people to radicalize Canadians or by those who seek to do harm to Canada. That's not something unique to TikTok. It's generally done across social media platforms.

The concerns that tend to be particular to TikTok have to do with the regime that it can operate under, because it is hosted and controlled, in theory, by China and their national security laws. We know that one important factor for data is how it can be used, and in Canada and other countries there are differing privacy protections. There's legal recourse in Canada and we have charter protections. Many things are inherent in our country that are not the same in China.

Mr. Matthew Green: From your review, do you have any evidence or intelligence you're able to share publicly that would indicate TikTok has broken any Canadian laws?

● (1745)

Mr. Daniel Rogers: In our review, we were clear in the decision-making process that the national security concerns related to TikTok Canada were an element of our decision-making. I can't speak to specifics on those, but I will say that we don't require TikTok to have broken Canadian laws for us to have national security concerns and—

Mr. Matthew Green: I'm sorry. My time is limited, so I have to take it back.

Do you have concerns about other platforms, such as, for instance, Truth Social, X, Discord and WhatsApp? We're talking about this in hopefully a more comprehensive way than just targeting one platform. Would you care to comment on the threats for radicalization, as you've mentioned numerous times at committee, from the other platforms?

Mr. Daniel Rogers: Our concerns around the spread of information and radicalization are not specific to a particular platform, nor have we, at least to my knowledge—I've only been the director for six weeks—conducted a similar review of any of those platforms at this stage, certainly not as part of the ICA process. As I've said, our concerns are more to do with content and the potential for Canadians to be radicalized on those platforms—

Mr. Matthew Green: Define “radicalization”. You use the term, but what does it mean legally?

Mr. Daniel Rogers: Thank you for asking. In our context, that typically means.... I use it as shorthand for “radicalization to violence”.

There is a threshold. People are allowed to have freedom of expression in Canada. People can say what they wish on social media, and they can consume the information they wish, but radicalization, for us, is the process that someone goes through to take what are beliefs and translate them into the intention to commit violence and harm people here in Canada.

Paul, I don't know if you have anything else you want to add on radicalization.

Mr. Paul Lynd: That's essentially accurate: It's mobilizing towards providing support to violence or conducting a violent act.

Mr. Matthew Green: What are some examples of that in Canada recently?

Mr. Daniel Rogers: Well, you've probably seen a number of arrests relating to individuals who have espoused radical ideologies and may have been planning attacks—in some cases youths. Examples of that include people who live in an echo chamber online and may have fewer connections outside to temper what they—

Mr. Matthew Green: Those aren't examples. Those are generalities. To be specific, I mean the Quebec City massacre at the mosque, the Ibrahim Jame mosque in Hamilton, which was firebombed, and the London family that was run down. Would those be specific examples of radicalization?

Mr. Daniel Rogers: I don't want to get this wrong. I won't use the name, but I certainly know that some of the arrests that have been made this year have been linked to radicalization online as a primary factor. I don't want to give you misinformation and give you the wrong name associated with that, but I'm happy to report back if that's helpful.

Mr. Matthew Green: If you're able to, can you list, in the case of TikTok, the principal national security risks that you identified that led to the Government of Canada's decision to order it to wind up?

Mr. Daniel Rogers: I can't speak to specifics other than to say that we provided a national security assessment that highlighted some national security risks.

Mr. Matthew Green: Okay. What are the risks of disclosing to this committee, publicly, some of this information?

Mr. Daniel Rogers: Well, for one, there are decision-making privileges in cabinet confidence that we have to respect as part of the government's decision-making. Also, there is a matter before the courts that will have to go through a fair process, and I need to be conscious that this process hasn't yet unfolded. There may be classified information that could reveal sources or techniques or may have been shared with us by our allies, who would not allow us to describe it publicly.

Mr. Matthew Green: Obviously, under the CSIS Act, you have a duty of candour to the courts. If in the process of the civil case you're asked these questions, you'll be forced to disclose that. Is that correct?

Mr. Daniel Rogers: I can't offer specific legal advice. I know there are processes to protect information in various legal proceedings in Canada, which may be applicable in this case. I have not done a detailed review of how this case might unfold and what information might come to light.

The Chair: Thank you, Mr. Green.

Thank you, Mr. Rogers.

That concludes our first round. I'm sure there will be lots of eyes on this court case.

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

Mr. Michael Barrett: With respect to the decision that was taken under the Investment Canada Act, what alternatives or other options are available other than a complete shutdown of an entity here in Canada?

● (1750)

Mr. Daniel Rogers: Some of those questions may be better directed to ISED, which applies most of the act. Again, our input is limited to providing a national security assessment.

That said, I understand there are other options available, including applying mitigation mechanisms, but I wouldn't want to speak about that on their behalf.

Mr. Michael Barrett: Is there a type of mitigation example you could offer?

Mr. Daniel Rogers: None comes to mind right away. I apologize, but that's not CSIS's area of expertise with the act.

Mr. Michael Barrett: There's a national security risk so great that, under the Investment Canada Act, the headquarters of this entity has been ordered to shut down in Canada, yet Canadians are not restricted in their use of it. What are Canadians to make of this? The risk is so great that the government ordered the shutdown of this entity but said, “Please feel free to continue to use the app.” What's the message Canadians should take away from that?

Mr. Daniel Rogers: From CSIS's perspective, we've been clear, as I have been now, about the risks of the app itself.

Mr. Michael Barrett: Can you be clear? Should Canadians continue to use TikTok?

Mr. Daniel Rogers: We have said, and I will say now, that there are national security concerns with the use of TikTok in general, including with the aggregate amount of data and the ability of the Chinese government to make use of the platform in ways that are contrary to the interests of Canada.

Mr. Michael Barrett: Are you saying that Canadians should use it or should not use it?

Mr. Daniel Rogers: I'm saying that the decision of a government to provide such a recommendation to Canadians, or make a decision for them, is best not made by CSIS.

CSIS can provide a national security assessment, but it's very important that other factors be brought into those decisions. The decision on TikTok Canada is very distinct from the decision on TikTok in general, because there are very different factors at play.

Mr. Michael Barrett: As to the distinct question of whether individual Canadians.... I'm not talking about a ban. I'm just talking about advice. You're the director of the leading organization in Canada's intelligence apparatus. You are at the forefront of this and, though new in your role, you were appointed because of your qualifications and extensive experience in the intelligence community in Canada.

Should Canadians continue to use TikTok? I'm not asking whether the government should ban it for Canadians. I'm asking if, as the head of CSIS, you believe it's wise for individual Canadians to use it.

Mr. Daniel Rogers: I think there's a very big distinction between an individual's choice to use something and the aggregate effect on Canadian national security.

I can give you a personal example. When I was young, I did not expect to be the director of CSIS. At the time, I may have looked at the information available to me and made a decision to continue to use TikTok because I wouldn't have thought I'd care, even if China had my information. I now care because I'm the director of CSIS.

My perspective is that individuals need to consider their own risks. That is an important factor in making a determination. At this stage, I can't speak for government, but I can say there are risks that I hope Canadians consider when they personally decide to use TikTok.

Mr. Michael Barrett: You talked about the aggregation of data—the information, pictures, geolocation, patterns and habits of individual Canadians. That information is being taken, potentially used by the Communist dictatorship in Beijing and aggregated.

I have just about a minute left.

With respect to individual users, what are the risks to younger Canadians—the young Mr. Rogerses and future directors of CSIS—in 50 seconds, sir?

Mr. Daniel Rogers: If the concern is that the Chinese government may access data, they have been seen, as we know, engaging in foreign interference, in acts of transnational repression and in other things contrary to the individual and collective interests of Canada. An individual making use of TikTok now would have to be aware that their data may be subject to that regime.

If you are someone who is vocally counter to the Government of China or the Chinese Communist Party, you may have particular concerns immediately. If you are someone who is not in that situation, you may eventually have those concerns, and you'll have to take into account as an individual whether you want to take that risk.

Mr. Michael Barrett: I hear concerns from locally owned businesses in my community that sell their products in Canada using TikTok. What do I say to them? Should they also be concerned?

Mr. Daniel Rogers: I think the same advice applies. The data and use of TikTok will be available through the regime we've described. They'll have to make those decisions.

● (1755)

Mr. Michael Barrett: Thank you.

The Chair: That was a good discussion, Mr. Rogers.

Just to let everybody know, I'm going to Mr. Bains for five minutes.

[*Translation*]

Mr. Villemure and Mr. Green will have two and a half minutes each.

That will conclude our meeting.

[*English*]

I see a thumbs-up from Mr. Green.

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

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

Thank you to our security intelligence representatives for joining us today.

I'd like to take a moment to thank you for your work, your proactive efforts in community engagement and your work with respect to Bill C-70, specifically on strengthening the Foreign Interference and Security of Information Act, something that hadn't been done in over 20 years. I want to thank you and the department for your efforts there.

I want to start by stating that prolonged operations by TikTok could allow foreign actors to exploit Canadian user data or spread disinformation. Is this an accurate statement in your mind, Director Rogers?

Mr. Daniel Rogers: I think I missed the beginning of your question.

I think you asked whether TikTok could allow for the spread of disinformation. Yes, that's true, and it's also true of other social media platforms.

Mr. Parm Bains: Specifically, I said that the operations by TikTok could allow foreign actors to exploit Canadian user data and spread disinformation. Is that accurate?

Mr. Daniel Rogers: Yes, that's accurate.

Mr. Parm Bains: In terms of providing guidance on timelines for winding down the activities of TikTok to minimize potential risk to public safety and our democratic integrity, what has CSIS done?

Mr. Daniel Rogers: Our role is to provide advice to the government in that regard. We've provided advice on a number of decision points, including the most recent one to wind up TikTok Canada.

We also collect intelligence, obviously. Where we can collect intelligence that informs the government on how social media platforms are used by foreign adversaries or anyone who would seek to undermine the security of Canada, we do that, and that classified information would factor into future government decisions.

Mr. Parm Bains: Just going back to what my colleague Mr. Barrett raised about having the physical presence of TikTok on Canadian soil versus concerns about the app, can you distinguish the difference between those things?

Mr. Daniel Rogers: Yes. As has been pointed out, the app itself can continue to run independent of the presence of TikTok Canada.

Mr. Parm Bains: Is there a difference in risk between having them here...? Is it important for us not to even have them on our soil versus the app itself? I understand they can continue to produce information, take data and use algorithms to scrape people's information on what they're doing, but that's the question.

Mr. Daniel Rogers: The review of TikTok Canada individually did raise some national security concerns that were unique to that transaction. In the context of the Investment Canada Act, we review the transaction itself, and that was factored into the government's decision at the time.

Mr. Parm Bains: You talked about our allied partners, the Five Eyes. The government has aligned itself with our allies in recognizing the risks posed by TikTok.

How does CSIS assess Canada's response to these risks compared to that of our allies? What are they doing? Are you all exchanging information to say what is working and what is not working?

Mr. Daniel Rogers: It's a very good question. Each of our allies has different regimes for reviewing investments and for placing controls on applications and has other sorts of legislative frameworks. It's not a one-to-one comparison.

For CSIS, our primary activity is to make sure we share and compare intelligence and assessments with our Five Eyes allies. This includes the activities of, for instance, China and others as it relates to the use of social media platforms like TikTok and, I suppose when possible, where mitigation measures have proven effective by doing intelligence collection.

Mr. Parm Bains: TikTok is based out of China. It's a Chinese company, but it's being used by billions of people. Are you able to identify certain hostile nations using it more than others?

● (1800)

Mr. Daniel Rogers: I'll invite my colleague to jump in if he knows more than I do.

We've certainly seen foreign actors use many social media platforms, including TikTok. We've been fairly public about concerns with disinformation, misinformation and influence done by Russia, China and others.

Paul, do you want to add to that?

Mr. Paul Lynd: Sure.

I would say the concern with TikTok is specific to its association with the PRC. As mentioned here, TikTok collects a lot of personal data and has access to a lot of personal data on your device. CSIS has been very publicly warning about the risks of using TikTok. It's very clear that there's a strategy on the part of the PRC to collect big data and personal data from all around the world.

The PRC is also the primary threat actor in Canada connected to foreign interference. When you have a vast amount of collected personal data and on top of that have AI and machine learning that you can use to sort through that data and use it against people, you can use it for foreign interference, to target individuals, for cyber-attacks, to intimidate, to influence and to compromise in the future.

Really, the concern is the vast access that TikTok allows to personal data and the fact that the PRC's national security laws would compel it to share that data.

Mr. Parm Bains: Thank you very much.

The Chair: Thank you, Mr. Bains. I felt it important that Mr. Lynd answer that question, so you had a lot more time than normal. It was an important response.

Thank you, Mr. Lynd.

[*Translation*]

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

Mr. René Villemure: Two and a half minutes isn't very long.

Have we seen an increase in interference activities by the Chinese government here in Canada?

[*English*]

Mr. Daniel Rogers: We certainly see continued foreign interference by the PRC here in Canada. It has been spectacularly public over the last little while and it concerns CSIS. We are concerned about it specifically in the context of the potential use of social media to provide narratives beneficial to the PRC that may be disinformation or contrary to Canadian interests.

[*Translation*]

Mr. René Villemure: You were talking about radicalization a little earlier. I've often read that the Chinese government's goal was to create chaos through false stories.

Do you see a resurgence of certain themes, such as religion, for example? What are the current themes?

Mr. Daniel Rogers: You may want to add something about themes, Mr. Lynd.

[*English*]

I think China is particularly seeking to ensure pro-PRC narratives across the community. That's something we've seen fairly regularly. It's not necessarily about causing chaos, but about promoting a narrative that serves its own interests, whether to make it more appealing to Canadians to follow a Chinese perspective, which may be contrary to Canadians' interests, or to try to influence in particular the Chinese diaspora here in Canada.

Paul, is there anything you want to add?

Mr. Paul Lynd: All I would say is that their primary focus is to protect the Chinese Communist Party. What we're most concerned about, from a CSIS perspective, is foreign interference in Canada and them trying to achieve objectives for their own foreign policy in Canada.

I don't have details handy for the different themes of what they've been involved in, but our concern really is foreign interference in Canada on behalf of the PRC.

[*Translation*]

Mr. René Villemure: Do you see a difference in the use of English, Chinese or French, for example?

Mr. Daniel Rogers: That's a good question. I don't know if the Chinese use French or English more in Canada. I know they use any technique to effectively reach the majority of Canadians.

[*English*]

In general, there's a much more substantial English ecosystem in the United States, for example, which tends to have an effect on English-speaking Canadians or French-speaking Canadians who consume English media.

[*Translation*]

Mr. René Villemure: Thank you very much.

The Chair: Thank you, Mr. Villemure.

[*English*]

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

Mr. Matthew Green: Thank you very much.

Perhaps the director can answer a question that TikTok itself couldn't answer, or at least wouldn't even entertain. From your perspective, why should I as a member of Parliament not be on TikTok?

Mr. Daniel Rogers: That's an excellent question.

The risks I mentioned earlier in one of my responses apply especially to members of Parliament, who may find themselves of interest to the Chinese government as a target of their influence. If your data is on TikTok and China avails itself of that data, it may seek to understand more about you, more about your personal networks and more about the ecosystem that you work in to be able to target foreign interference, espionage, cyber-attacks or other things toward you.

Obviously, as members of Parliament, you have a particular access to and influence with the government that most people don't enjoy, and I can imagine why you would be a particularly interesting target for the Government of China.

● (1805)

Mr. Matthew Green: How is that different from the other platforms? Presumably we're in surveillance capitalism, setting aside the state capitalist country of China. What's to say the Chinese, Indian, Russian, Israeli or American governments couldn't simply buy that information directly from Meta, X or any of the other actors that provide these types of platforms?

Mr. Daniel Rogers: That's another good question.

I would certainly not say that TikTok is the only concern we have with respect to Chinese access to data and its influence activities. It is one of the things we're concerned about, particularly given the potential for its national security law to apply directly to a company headquartered in China.

One of the primary differences between TikTok and others and between China and others is that China has shown a history of engaging in foreign interference activities specific to Canada. It has a very sophisticated and capable cyber-program for intelligence collection and espionage. It tends to be the number one cyber-actor prominent in Canada. With respect to which government, I think China has distinguished itself in a number of ways.

Mr. Matthew Green: Does your threat assessment change if the same types of activities are being observed by an “ally”?

Mr. Daniel Rogers: I think CSIS's act and mandate are not country-specific. We look at anything that meets a national security threshold for us and is contrary to Canada's national security interests. Right now, that certainly includes the PRC and tends not to include our allies.

Mr. Matthew Green: Wouldn't it be rational to think we're more influenced by American media and American information than we are by other foreign actors?

Mr. Daniel Rogers: As I mentioned earlier, the targeting of disinformation by certain foreign actors toward an American ecosystem has knock-on effects for Canadians who consume information in that ecosystem also.

Mr. Matthew Green: That's interesting. That wasn't exactly the question I asked, but it's an interesting response. Thank you very much.

I know my time is up, but I'll just say, Mr. Chair, that I still have more questions than we have answers on this. I would really appreciate any information from Mr. Rogers, even if it's at the direction of an in camera briefing. As an opposition member, I feel—and I'm not saying this as a question of privilege, but I'll put it out there—that we still don't have all the information to provide any real analysis on this.

Thank you very much.

The Chair: Thank you, Mr. Green.

On that point, I would leave to your discretion and that of other committee members how you want to handle this. The motion passed by the committee was to deal with this in the manner in which we are. Specific requests for witnesses were placed before us, and we're doing everything we can through the clerk to make sure we have those witnesses in front of us. I'll leave to your discretion which way you want to go with this.

We're still trying to get a hold of Mr. Vigneault, the former director of CSIS. Also, as I mentioned, I did invite TikTok. They weren't part of the motion, but I thought they were germane to the study. They respectfully declined given, I assume, the circumstances they're now facing with the civil case.

I'm reminded that there's the minister as well, who has indicated to us that he will be available at the end of January. I think that will be an interesting meeting. We'll see what we can do to get everyone here.

I don't have any other business, so Mrs. Shanahan, go ahead.

Mrs. Brenda Shanahan: Are you planning a meeting for the 17th?

The Chair: I'm leaving it open right now. I will give an indication to the committee. It's a very difficult proposition for me to just say no at this point. I don't know what's going to come up. You'll have an advanced warning. I understand that there's an event that night that you need to be at.

● (1810)

Mrs. Brenda Shanahan: I have a party to plan.

Some hon. members: Oh, oh!

The Chair: Mr. Lynd and Mr. Rogers, I want to say, on behalf of the committee, congratulations on your appointments. I can't imagine the work you have in front of you. This committee has been engaged on and involved in the issue of foreign interference, disinformation and misinformation, which I'm old enough to remember used to be called lying. You certainly have a challenge ahead of you.

I want to thank you on behalf of the committee and Canadians. Again, I congratulate you on your appointments. Thank you for being here today and for dealing with the questions of the committee.

Mr. Daniel Rogers: Thank you very much. It was a pleasure to be here.

The Chair: That's it. Have a great weekend, everyone, and safe travels.

The meeting is adjourned.