HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

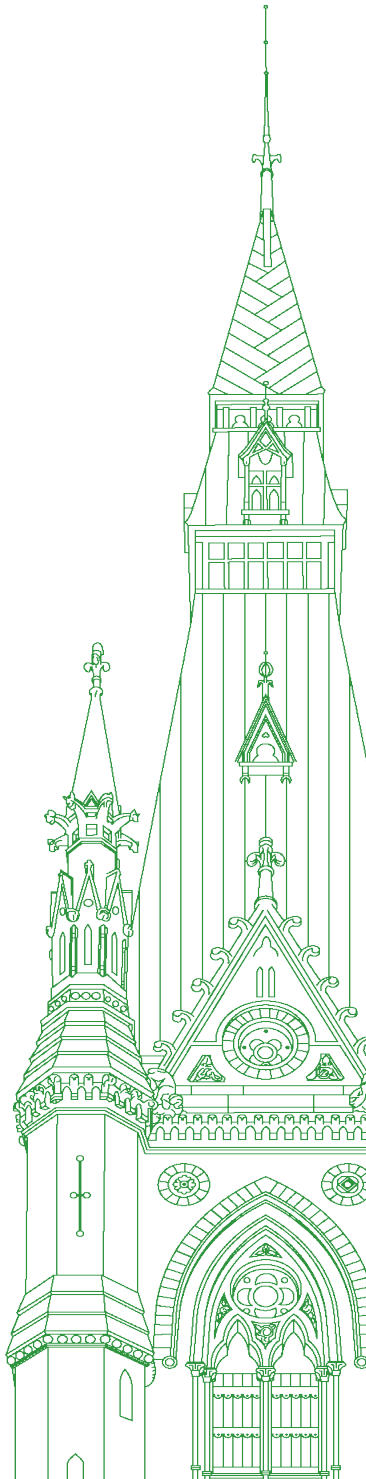
43rd PARLIAMENT, 1st SESSION

Standing Committee on Procedure and House Affairs

EVIDENCE

NUMBER 012

Wednesday, April 29, 2020



Chair: Ms. Ruby Sahota

Standing Committee on Procedure and House Affairs

Wednesday, April 29, 2020

● (1705)

[*English*]

The Chair (Ms. Ruby Sahota (Brampton North, Lib.)): I call this meeting to order.

Welcome to meeting 12 of the House of Commons Standing Committee on Procedure and House Affairs. Pursuant to the order of reference of Saturday, April 11, the committee is meeting to discuss the parliamentary duties in the context of the COVID-19 pandemic.

Before we start, I want to inform members that pursuant to this order of reference, the committee is meeting for two reasons: one, for the purpose of undertaking a study and receiving evidence concerning matters related to the conduct of parliamentary duties in the context of COVID-19; and two, to prepare and present a report to the House by May 15 on the said study. The order of reference also stipulates that only motions needed to determine witnesses, and motions related to the adoption of the report, are in order.

Today's meeting is taking place via video conference. The proceedings will be made available via the House of Commons website. Just so you are aware, the webcast will always show the person speaking rather than the entirety of the committee on that webcast.

In order to facilitate the work of our interpreters and ensure an orderly meeting, I would like to outline a few rules to follow. Interpretation in this video conference will work very much like it does in a regular committee meeting. You have the choice, at the bottom of your screen, of the floor, English or French channels.

Before speaking, please wait until I recognize you by name. When you are ready to speak, you can either click on the microphone icon to activate your mike or hold down the space bar while you are speaking. When you release the space bar, your mike will mute itself, just like a walkie-talkie. When you have it pressed down, you're able to speak. When you release it, you'll be back on mute.

I would remind you that all comments by members and witnesses should be addressed through the chair. Should members need to request the floor outside of their designated time for questions, they should activate their mike and state that they have a point of order. If a member wishes to intervene on a point of order that has been raised by another member, they should use the "raise hand" function. This will signal to the chair your interest to speak. In order to do so, you can click on "participants" at the bottom of your screen. When the list pops up, you will see that next to your name you can click the "raise hand" function. It might also be at the bottom of your participants list.

When speaking, please speak slowly and clearly. When you are not speaking, your mike should be on mute. The use of a headset is strongly encouraged.

Should any technical challenges arise—for example, in relation to interpretation or a problem with your audio—please advise the chair immediately, and the technical team will work to resolve them. Please note that we may need to suspend during these times, as we need to ensure all members are able to participate fully.

Before we get started, can everyone click on their screen in the top right-hand corner and ensure that they are on gallery view? With this view, you should be able to see all the participants in a grid view. It will ensure that all video participants can see one another.

During this meeting, we will follow the same rules that usually apply to opening statements and the questioning of witnesses during our regular meetings. As per the routine motions of the committee, each witness has up to 10 minutes for an opening statement, followed by the usual rounds of questioning from members. However, due to the size of the witness panel, I am asking that all witnesses be as brief as possible in their opening statements in order to allow as much time as possible for questions by the committee members. Just as we usually would in a regular committee meeting, we will suspend in between panels in order to allow the first group of witnesses to depart and the next panel to join the meeting.

I'd now like to welcome our witnesses.

We'll start with Ms. Qaqqaq. I believe, if we do not have Ms. Ashton here yet.

Let's hear from Ms. Qaqqaq, please.

Ms. Mumilaaq Qaqqaq (Nunavut, NDP): *Mat'na*. Thank you for having me.

I understand that we have some time limitations. I had provided a couple of pages of briefing notes, so I'll try to go through them as quickly as I can.

Thank you for giving me the opportunity, first and foremost, to speak at this committee. My name is Mumilaaq Qaqqaq. I'm the member of Parliament for Nunavut. Nunavut is Canada's youngest territory, and I'm proud to be the youngest person elected in the riding, and one of the youngest voices in this Parliament as well. Nunavut is also the largest electoral district in the world, with a population of approximately 39,000.

I was raised in Baker Lake, a growing community of 2,000. I now live in the capital of the territory, Iqaluit, which has a population of about 8,000. All 25 communities in the riding are fly-in and fly-out, with no roads to connect families and people across communities. Approximately 85% of my constituents are Inuk, or Inuit.

I am currently speaking to everybody here on the committee from Ottawa. I can't confidently say I could participate in a virtual Parliament or a virtual committee if I were actually in my riding. Connectivity is essential.

Unfortunately, our territory has the highest suicide rate per capita in Canada. This has tragically been the case for years. I grew up with this being perceived as our normal, which is wrong. I have lost countless friends and family to suicide. Everyone in the territory is, in some way, touched by suicide. This reflects the social determinants for individuals in the territory.

One-third of my constituents live in overcrowded homes. We also know that seven out of 10 children go to school hungry in Nunavut. There are communities that continue to see boil water advisories and limited access to clean drinking water. We have some of the highest living costs in the country. Along with investments in housing, building basic infrastructure is a must in the territory. Connectivity is essential.

Accessing critical and often life-saving information is frequently a challenge in Nunavut. Providing individuals with key information in their mother tongue, Inuktut, can be life-saving. In 2016, 23,225—approximately 65% of the population—reported Inuktut as their mother tongue.

I was glad to see during the previous parliamentary session an announcement that talked about a commitment of $42 million over the next five years to support Inuktut language initiatives. This was a collaboration among the Government of Canada, the Government of Nunavut and Nunavut Tunngavik Incorporated, the territorial advocacy organization.

Although the intentions of this agreement are good, I face many barriers as a member of Parliament in providing needed translation to my constituents. For example, I would need to translate all my work five times to make sure information is easily available to everyone. Guiding constituents to the federal services they need is a similar obstacle. Providing translation in Inuktut at the federal level for my constituency and other Inuit Nunangat communities would be nothing but beneficial for everyone. Connectivity is essential.

As we saw during yesterday's committee, even in some of the most prosperous parts of the country, technical limitations are impacting parliamentarians' ability to do their work. I thought it was important for everyone here at the committee today to get a sense of the Internet speeds here in Ottawa compared to communities in Nunavut. I reached out to some constituents and asked for their Mbps, or megabits per second, and was frustrated, but not surprised, by some of the numbers that I heard. For example, I did my own testing here in Ottawa. With my phone plan I have 180 megabits per second, and with my Wi-Fi I have 200 megabits per second. Please keep in mind that you need at least eight megabits per second to run a high-definition video conferencing call, and these results will be impacted if you are sharing a network with other people.

● (1710)

These are some of the constituent responses I had. I tried to hit all three of my regions. In Cambridge Bay, we see Wi-Fi at 14 megabits per second, and data at 51. In Baker Lake, my hometown, Wi-Fi is again at 14 megabits per second, and data is 85 megabits per second. Arviat's Wi-Fi is at six megabits per second and data is at 51 megabits per second. Sanikiluaq Wi-Fi is at two megabits per second, and data in Sanikiluaq is at 13 megabits per second. Connectivity is essential.

This isn't part of my notes, but earlier this afternoon during the session, a minister thanked the member for a question on the issue of rural broadband in his region. We know that before the COVID-19 crisis began the government recognized that fast, reliable and affordable high-speed Internet was a necessity, not a luxury, so clearly the federal government knows that this is a problem.

We continue to see large corporations like Bell charge ridiculous prices across Canada. Everyone here would agree that hours and hours of streaming parliamentary business on their data plans could result in some outrageous overage charges. During this crisis, we have also heard stories of cellphone and Internet providers suddenly charging Canadians more. How can we ask families to stay at home, parents to continue working and students to learn through online resources without providing affordable and accessible Internet services?

When I say this, I want you to keep in mind the fundamental human rights issues I have previously mentioned that too many of my constituents—Nunavummiut, Canadians—are facing.

Northwestel, one of the major telecom companies in Nunavut, has fortunately provided temporary Internet usage relief until May 31 for existing customers, which is one way we should be taking care of each other right now. Connectivity is essential.

With this in mind, I would like to talk about the proposed Kivalliq hydro-fibre link. I would like to echo the words of Premier Joe Savikataaq when he said, “The proposed Manitoba-Nunavut hydroelectric power line transmission and fibre optics project aligns with our Turaaqtavut mandate, Nunavut's growing telecommunications needs and the Government of Canada's goal to reduce the effects of climate change.”

The Kivalliq hydro-fibre link is an opportunity not only to promote cleaner energy but to provide much-needed Internet and data supports for our communities. We have yet to see the support needed from the federal government for this project. Connectivity is essential.

The amount of needed services in Nunavut is extremely high. Increasing accessible and affordable connectivity services could save lives. We could promote online counselling, education resource exchange, share information with one another and do so many other beneficial things.

Again, I'd like to thank everybody for this opportunity. I hope I was able to capture the basics of the reality in my riding and why connectivity is essential. There is much opportunity for us to do great things and provide these services to the people who need them.

Mat'na. Thank you.

● (1715)

The Chair: Thank you, MP Qaqqaq.

Next we will hear from MP Ashton, please.

Ms. Niki Ashton (Churchill—Keewatinook Aski, NDP): Good afternoon, fellow colleagues. Thank you for having me as a witness today.

It's unusual to be on this side of the table, or the screen, as a witness at this committee. I truly value the opportunity to share the perspective of many in our region as your committee finds ways to make virtual Parliament work.

First, I want to be clear: I am a proponent of a virtual Parliament. I spoke out publicly about the need for a virtual Parliament early on in this pandemic. I also spoke out about the need to make Parliament more accessible, including virtually, for some time, even before this.

Currently, we are living in an unprecedented time of crisis. Many Canadians have had to take unprecedented steps to stay safe: physical distancing, working from home if possible, and juggling full-time parenting with work. For others, including essential workers, staying home is not an option. Many are dealing with the crisis of losing their jobs.

Throughout this time, our work as representatives and advocates has, if anything, become even more important. Over the last number of weeks, I've been in close contact with first nations leaders in our region who are doing everything they can to keep their communities safe, desperate for federal action. I've been in touch with front-line workers who don't have enough access to the personal protective equipment they need. I've been in touch with workers in work camps and mines across our north who are afraid to go to work because of a possible spread of COVID-19. I've been in touch with constituents stranded abroad, students who don't know how they'll pay their rent and seniors who are in need of support.

Our work has not stopped, but without Parliament and access to the accountability mechanisms that are integral to it, our ability to make change has been deeply impacted. Like many of you, I've been in contact with ministers, parliamentary secretaries and the media, doing everything possible to get action for our region. That is important, but fundamentally we are members of Parliament. Canadians expect us to represent them in Parliament, whether we are in government or in opposition.

Let's recognize that at a time when people who can are encouraged to work from home, we should be doing that too. For reasons of public health, we shouldn't be any different. We should be setting a high bar to show that it is possible to do a wide range of work remotely, including the work of Parliament. Let's be responsible in terms of our work. When we are told that we could be supercarriers of COVID-19, let's do everything possible to do our work safely from home.

Research has indicated that we could be dealing with future, and possibly multiple, waves of the coronavirus. This isn't a matter of weeks, but months and even years. We must be seen as leaders in terms of public health and do everything we can to keep our communities safe, including refraining from travelling across the country on a regular basis when we could be doing this work from home.

Right now, here in my home region, we have a travel restriction where people who do not live north of the 53rd parallel are not allowed to come in unless they work here. Non-essential travel is not recommended. These are public measures reflective of how vulnerable our region is. There are also widespread public health recommendations to avoid interprovincial travel. Given our work as leaders, we must go above and beyond to keep our communities safe and do our work from home.

A virtual Parliament is critical in terms of regional representation. Until now, no Manitoba MPs from any party have attended an emergency sitting of Parliament. We know that, again, for public health reasons, emergency sittings and the in-person sitting today are dominated by MPs from central Canada, those who are near Ottawa. This is not acceptable. A virtual Parliament is critical in terms of gender representation. Based on research by Samara Centre for Democracy, it has been noted that the percentage of women in the House during emergency sittings has ranged from 25% to 27%. While reflective of our general representation, which remains pathetic, the fact is that a virtual Parliament can allow for women MPs to be heard across the country and for parties to ensure that their voices, our voices, are heard.

Let's also recognize that other jurisdictions have taken on this work already and put in place parliamentary sittings virtually: jurisdictions such as Wales, the U.K., the European Parliament, Ukraine, Argentina, and the list goes on. However, in setting up a virtual Parliament, we must recognize that we are not equal as MPs. Our region here in northern Manitoba, like much of rural and northern Canada, has extremely poor access to the Internet.

● (1720)

The Winnipeg Free Press recently reported on the fact that, according to the CRTC, Manitoba has some of the slowest Internet speeds in Canada. A CRTC map of broadband coverage shows major gaps across our province. An internal briefing note prepared by Industry Canada noted that as of 2018, “Northern Manitoba has the worst connectivity in all of Canada.” Nationally only 27.7% of first nations and 37.2% of rural communities have access to fast, reliable Internet.

This crisis is exposing the second-class access to critical infrastructure that many on first nations and in rural Canada are living right now. It is exposing a glaring and growing inequality in our country. It's having a negative impact on our kids, kids who already face immense barriers.

A CBC report recently made it clear that for first nations kids in remote communities like Garden Hill, here in our region, online learning is simply not possible. Catherine Monias, Garden Hill's education director, said when asked about offering online learning, “We can't...Most students do not have access to a computer and a printer, and most students do not have internet at home.” Even if there were more access to the Internet, Ms. Monias pointed out, “Our internet bandwidth is so narrow, that it's impossible to [teach online].”

I have heard from worried parents, frustrated educators and leaders from our region who are concerned about their young people's ability to access an education. We cannot have a situation where a generation of kids is held back because of our failures.

My office and I have also heard directly from constituents who have no access or unreliable access to the Internet when it comes to applying for EI, the CERB or getting help from Service Canada.

This cannot stand, and we must be clear that it didn't just happen. Successive governments' choices to fund private enterprise in the hope of providing broadband have failed. Good public money has been poured into initiatives that have not solved the problem. Years of Conservative and Liberal promises to ensure access to broadband Internet have failed. We've heard the campaign commitments and seen the posters, but there is no Internet.

I know of one community in our region that accessed the federal funds some years ago to build a tower, only to have the tower bought out by our main telecom provider and then dismantled. To this day, they do not have access to broadband Internet.

It's 2020, and in one of the wealthiest countries in the world, we face a shocking and unacceptable digital divide. This pandemic crisis should be a wake-up call. We need the government to recognize access to broadband Internet as a public good, a basic necessity, an essential service. The government must use public ownership to ensure the construction of broadband Internet infrastructure and ensure regulated and affordable service. It should also work with first nations and indigenous communities.

Many have compared dealing with this crisis to a wartime effort and said that we should be looking within to provide what we need. We are an incredibly wealthy country. Let's respond to the urgent needs of people at this time and into the future through national action now to ensure equal Internet access for all.

Let's come out of this crisis better than we were. Let's build a Canada where we are not letting down the next generation, and where we are not contributing to growing inequality. Canadians, including the youngest among us, are counting on us to do this. Let's get it done.

● (1725)

The Chair: Thank you, Ms. Ashton.

Next can we have Chantal Bernier, please?

[*Translation*]

Ms. Chantal Bernier (National Practice Leader, Privacy and Cybersecurity, Dentons Canada, As an Individual): Thank you, Madam Chair. I'm very pleased to be taking part in your work on this very relevant issue.

My name is Chantal Bernier. I'm a lawyer who specializes in privacy and cybersecurity law.

You invited me here today to outline the information security considerations associated with a potential virtual sitting of the House of Commons. I understand your concerns, particularly in light of media reports regarding security risks related to certain platforms. However, these risks must be put into context. First, they apply only to certain types of information. Second, they apply only to confidential debates. I'll address these distinctions.

[*English*]

In relation to the types of information you must protect by law as a public institution, there are two that are most relevant to your work.

The first category of protected information I will mention is information received in confidence in relation to the affairs of the Government of Canada, or received from another government, because the disclosure of that information would be injurious to the interests of the Government of Canada.

This type of information would never arise in the House of Commons. Should it arise in committee meetings, the committee should go in camera, and then the chair should ensure additional information security measures are applied, proportionate to the sensitivity of the information involved. The chair should not proceed to an in camera meeting unless there is assurance from the technology experts of the House of Commons that it can proceed securely online.

As a former senior public servant who had to lock her device in a little box every time she attended cabinet meetings, I can assure you that the Government of Canada has a long tradition of information security.

The second category of protected information I will mention is personal information. Personal information is defined as information that relates to an identified or identifiable individual, meaning that even if the information can be related to an individual only indirectly, it is still personal information, and you must, by law, protect it.

However, there are exceptions that are relevant to your work. These are types of personal information that you do not have to protect.

The first is information about an individual who is or was an officer or employee of the government institution where the information involved relates to the function of that employee or office. You also do not have to protect the fact that an individual is or was a ministerial adviser or a member of ministerial staff, as well as the individual's name and title. As well, you do not have to protect information about an individual who is or was performing services under contract for a government institution when, again, the information relates to that contract. Finally, information relating to any discretionary benefit of a financial nature to an individual, such as the granting of a licence or permit, is also not subject to protection and can be disclosed.

In other words, the protection of personal information cannot undermine government accountability.

● (1730)

Moving, then, to the type of proceedings that call for security measures, sittings of the House of Commons and meetings of House committees, except when they must go in camera, do not create security risks. It's quite the opposite. Because House debates are always public and are accessible directly from anyone's computer at any time, moving online preserves the transparency of Parliament more than it creates information security risks.

While I'm here, I would like to bring to your attention real information security risks that have not made the news. I am referring to telework. Working remotely from our houses raises information security risks. I speak on the basis of practical cases I have seen.

The main risks are these. The first one comes from the fact that many of us share a home. Telework means that the arrangements must provide physical protection of confidential information. Not everyone has a house big enough to allow a separate room to work in. Measures must therefore be adapted to each physical setting to protect information on both paper and screen.

Government documents should never be transferred to personal electronic devices. These devices are not configured in accordance with government information security standards. Government electronic devices should also not be made accessible to anyone except the government employee to whom the device has been assigned, even for temporary use. The devices are most likely to contain documents protected by law, and access by an unauthorized person constitutes a breach.

While passwords are the basis of security on electronic devices, they become even more important in the context of telework, an environment where you are around people who know you very well and, therefore, could guess your password. It's not necessarily for nefarious reasons, perhaps only because they want to use the computer. Still, it constitutes a security risk.

Without the entry-exit controls of Parliament offices, screens should be set to lock automatically when they are not used for a set period. That set period should be as short as necessary, according to the circumstances. Privacy filters on a computer can be used to hide the screen or make it invisible to others.

Finally, I would caution you against the accidental use of one's personal email for professional use. In the home environment this confusion risk is higher.

[*Translation*]

In short, I want to both reassure you and caution you.

I can reassure you by putting into context the issue of information security as it relates to your work. Apart from when you must deliberate in camera, the Internet maintains the level of transparency that we all want in the House of Commons rather than creating an information security risk.

When you need to sit in camera, Madam Chair and your fellow committee chairs, you must ensure that all safeguards proportionate to the sensitivity of the information involved are applied.

Regarding my cautionary note, I strongly encourage you to speak to all the members of your team about the measures that they've taken to ensure the protection of information while teleworking.

● (1735)

Thank you for your attention. I look forward to answering your questions.

[*English*]

The Chair: Thank you.

Next we'll hear from Mr. Leuprecht, professor of political science at the Royal Military College of Canada.

[*Translation*]

Dr. Christian Leuprecht (Professor, Department of Political Science, Royal Military College of Canada, As an Individual): Madam Chair, thank you for the opportunity to appear before the committee. I look forward to answering questions in both official languages.

[*English*]

I will start with some ad hoc remarks about cybersecurity in the current context, and then pass to some broader remarks about the continuity of constitutional government in the context of an emergency and a crisis. I shall edit those remarks and I shall indicate to the translators the edits so that you have the full written version in front of you in both official languages.

With regard to cybersecurity, here are a few brief considerations.

The deliberations you are having are hard to mess with because they're in real time and they're open, so tricks like deep faking what somebody might be saying seems to me to be pretty hard and difficult to make effective. On the next panel, I know there's somebody who is going to raise concerns about the Zoom technology, but I actually think that this is not particularly relevant in the current context. Yes, end-to-end encryption is the gold standard, but in this case, we're talking about an open Parliament and open conversations, so if we have interserver encryption.... We want people to be looking in anyways. If our adversaries want to listen in and see what a resilient democratic conversation looks like, all the better.

No matter what tool you're going to use, all the tools have vulnerabilities and are somewhat insecure. Some are less secure than others, but inherently there's always an issue with regard to compromise. I actually think this is a misguided conversation. This points to technological determinism, and technology is not ultimately the issue. It's behaviour that's the issue. It's how we use the cyber domain, so we need to have a more human-centric conversation about cybersecurity.

Many of the measures technologically can be readily solved as your parliamentary administrators already have with regard to Zoom, by sending passwords separately and locking down meetings. Really, it's a matter of what conversations we can simply not have online because we have to assume the conversation is compromised. There's still a lot you can learn from the metadata, even if you have end-to-end encryption. For instance, are you logging in through a virtual private network when you're logging in as a member of Parliament?

The greatest risk is probably not the software but your personal device. Is it already compromised? What kind of device are you using? What mechanisms are you using to connect: hard-wired or mobile? Are you on an approved device? Is the device hard-wired on a secure network with unique key identifiers, with a KPI card? Are we routing the traffic through a Canadian network to ensure Canadian data sovereignty, or is it being routed the most efficient way?

All this is to show that we need to think in human-centric terms, including how our adversaries might be thinking about this environment and their intent, and not in tech-centric terms. It's about the human factors of cybersecurity. Humans are ultimately the greatest vulnerability, but they're also an underused asset.

I'll point to, in this conversation we're having, nine issues with regard to human factors and cybersecurity that we are all experiencing every day.

The first is societal issues: How do we ensure that our democracy and our institutions are adequately defended? How do we ensure that they are cyber-resilient? How do we adapt our democratic institutions and how do we ensure that we have evidence-based policies?

With regard to regulation, we want to think about how we protect privacy, how we increase transparency and accountability, and how we standardize cybersecurity.

In terms of behaviour, we want to think about criminal networks, about enabling the behavioural change by users, and about designing more usable machines and more usable interfaces.

This ultimately leads me to questions about the role of Parliament. Ultimately the underlying primary constitutional principle here is the principle of responsible government. It is about ministerial responsibility, first and foremost, during a crisis and an emergency. It is about holding government to account and it is, in the Westminster parliamentary system, about parliamentary supremacy.

What does this mean concretely? It means voting supply on spending, on accountability, but also on how we raise revenue. I'm deeply concerned about how Parliament had very little say in how we raised revenue. Usually we think of this as taxation, but what we have seen in recent weeks is the largest and most rapid expansion of government in the post-war era. It has imposed unprecedented intergenerational burdens. We have seen this previously. The percentage of the debt this year that is being taken up in new debt is roughly what it was in the early 1980s. It hobbled government for a generation and led to considerable fiscal challenges down the road, hamstringing governments.

● (1740)

What are the mechanisms that are being deployed to ensure the spending that we are taking up is the most efficient and the most effective? I'm deeply concerned, in the current environment, about the temptation of privatizing profits and socializing debt, including private debt. When we restart the economy.... People are already talking about infrastructure, but this is what some people have called the “she-cession”. Unlike in 2008, the people who are disproportionately affected are women, and they are women in precarious situations. Building lots of bridges, roadways and subways is not going to help them, directly at least.

How do we think about how we restart the economy? In all of this, Parliament has a very important role to play.

I shall now pass to my remarks. I shall read from the first page and then extract lines from subsequent pages.

This is the greatest test for the maintenance of Canada's democratic constitutional order in at least 50 years. It raises many important questions. What is the legitimate extent of the federal government's power during an emergency? Is the federal civil service that drives Canada's federal system for coordinated emergency response a boon or a bane during a complex multijurisdictional, prolonged emergency? Did the Prime Minister get the best advice? Was the Prime Minister aware that the World Health Organization has had a very troubled relationship with China since 1957? These challenges are not new.

What are the appropriate roles—before, during and into a recovery—of the executive, judiciary and legislative branches? To what extent can the executive abrogate civil and privacy rights in the public and common interest, especially if citizens' confidence were to falter? Metadata will be an important part for mobile devices in reopening, in particular aggregate metadata and understanding people's behaviour. These require conversations.

To what extent do the proximate failures of the Canadian government to protect the safety and security of its citizens at home and abroad expose distal failures and weaknesses in intelligence, strategic assessments, emergency preparedness, continuity of constitutional government and the civil service's capacity and commitment to provide the best possible impartial advice to the government of the day, along with weaknesses in the structures and institutions of the Government of Canada and constitutional governance? After all, many democracies have fared significantly better than Canada in the speed and agility with which they responded to the epidemic, without the massive expansion of the state to which Canada has had to resort at a cost of billions of dollars.

The underlying rationale for the answers to these questions needs to be transparent and intelligible. There are questions about proportionality and suitability of these measures, as well as the fundamental transformation of the social and economic role of the state and public sector, whose expansion in recent weeks is without precedent in the post-war era. There's no precedent within living memory for anyone in a position of leadership of how to govern in this crisis, so Canada's democratic institutional order is absolutely critical. It is insufficient simply to tolerate criticism. The resilience and superiority of the democratic way of life is at its best when objections to the way the state optimizes how to manage and contain societal risk are actively sought out, enabled, heard and reciprocated. Even during a crisis, the government's power should not be absolute, unchecked and without recourse.

The hallmark of constitutional democracy is that, even during an emergency, executive power is contingent: The people have recourse through their representatives in Parliament to check the executive. Under such extraordinary circumstances, what are the prerogatives of the legislature in holding the executive accountable within the prevailing ethical and moral framework?

I'll move on to the top of the next page.

For over three centuries, voting supply has been the bedrock principle of the Westminster parliamentary system [*Technical difficulty—Editor*].

● (1745)

The Chair: Sorry, we're having some issues there.

I just wanted to inform you that you have a little less than a minute left. Since you just indicated you were starting another page, I want to encourage you to try to sum up.

Thank you.

Dr. Christian Leuprecht: All right.

The events of recent weeks appear to validate the resilience, adaptability and vitality of Canada's constitutional system.

I shall be on the last page, for the translators, and I shall make my remarks quick.

The Government of Canada has long taken a laissez-faire approach to departmental emergency planning, which facilitates event-driven reactions, where the perceived urgency trumps the actual importance. I'm concerned about overzealous experts who want to outlaw certain types of behaviour without interventions from politicians. Ottawa mayor Jim Watson's intervention with regard to people actually being able to have a beer in the driveway while respecting social distancing is a good example.

Especially during a time of crisis, Parliament has a supreme duty to hold the executive to account. Canadians need continuous parliamentary audit of the executive and the bureaucracy's judgment.

During the First World War, high commands often found themselves at odds with national assemblies. Indeed, national assemblies had conceded extra powers to the executive branch and exercised restraint over the way their military prosecuted the war. Assuming the war would be brief, they deferred to experts and professionals, but in the wake of a succession of failed offences and military stagnation, parliamentarians demurred. They attempted to regain control of the war effort by injecting criticism and new ideas. Georges Clemenceau, when he became premier of France in 1917, famously surmised, “War is too serious a matter to leave to soldiers.”

Then I go through a series of issues where the British generals got it wrong and Winston Churchill got it right. Military strategy requires civilian perspective and leadership. That's what we learn from civil-military relations. To paraphrase Clemenceau, a pandemic is too important to leave to health experts or the executive alone, hence the importance of the role of Parliament. Never has it been more important than today.

The Chair: Thank you so much.

Next we have Monsieur Turcotte, director of the technology analysis directorate at the Office of the Privacy Commissioner of Canada. Thank you.

[*Translation*]

Mr. Martyn Turcotte (Director, Technology Analysis Directorate, Office of the Privacy Commissioner of Canada): Thank you, Madam Chair and committee members for the invitation to speak to you today.

You're currently studying ways in which members can best fulfill their parliamentary duties during the COVID-19 pandemic. You're looking at the temporary modification of your procedures and technological solutions to support a virtual Parliament. We've been asked to speak to you today about privacy issues related to web-based video conferencing platforms as you consider potential solutions.

At this time, we're all navigating and adapting to a new reality of social distancing. Many of us have turned to video conferencing services for both personal and professional use. Governments and parliaments around the world are also using these efficient and readily available platforms to carry out important work.

We often see a connection between the privacy concerns and the cybersecurity risks and vulnerabilities of these platforms. These types of digital solutions are widely available and seamless to use, which explains their surge in popularity. However, there have also been reports of privacy and security issues related to their use. These issues stem from flaws with end-to-end encryption and data collection or sharing practices embedded in the terms and conditions. Specific risks along these lines would be unique to each video conferencing service in question. Any tool has its pros, cons, strengths and vulnerabilities.

● (1750)

[*English*]

There is a good reason to be prudent when considering cybersecurity concerns or vulnerabilities with any particular technology option. There have also been reports that the COVID-19 crisis has created new opportunities and motivations for cyber-attacks, which only increases the importance of ensuring there are adequate safeguards in place to protect against unauthorized breaches of personal information.

As you consider various technological solutions to support a virtual Parliament during this pandemic, it will be important to bear in mind that certain solutions may not be equally suitable for all situations. Parliament should first determine its needs and then assess the technical safeguards, the potential security risks and the privacy policies of each service before selecting a particular platform.

For situations that would involve government discussions requiring secure communications, I would defer to our government cybersecurity experts to provide specific technical expertise on appropriate solutions to support the work of Parliament. I would only add that a self-hosted web-based video conferencing system solution is generally more secure than using a web-based video conferencing system offered by a provider, because there is more ability to control certain technical features and, therefore, to adapt it to your specific needs.

If options other than self-hosted solutions are being considered, such as the numerous web-based video conferencing services that are broadly available, they should generally be reserved for public matters only.

[*Translation*]

A number of measures can be taken to protect privacy even when a system is used for public meetings. In such cases, we recommend the following:

The committee should conduct a careful review of the video conferencing service's privacy policies and terms of use to understand the terms for the collection, use and disclosure of personal information and third party contractual arrangements.

When using a private messaging feature during a video conference, pay particular attention to whether the messages remain private. Some messages may form part of the transcript of the meeting, and thus ultimately be more broadly available than the author intended.

For public committee meetings or House debates, the host—or in your case the chair of the committee—can prevent “Zoombombing,” gate crashers or other unwanted activities by disabling certain features such as “join before host,” screen sharing or file transfers.

Members who participate in a video conference should be careful about their own environment, such as where they sit. The people and items visible in the background can reveal a great deal of information.

Lastly, if members are using a web browser to participate in video conferences, it would be best to open a new window with no other browser tabs. Ideally, they should also close other applications to avoid inadvertently sharing notification pop-ups—showing, for example, new incoming emails—with other participants and the video conferencing service provider.

The Office of the Privacy Commissioner of Canada is currently preparing a list of best practices for individuals to mitigate common privacy and security concerns associated with web-based video conferencing systems. However, on their own, these measures don't guarantee that all privacy and cybersecurity risks would be adequately addressed, particularly in situations requiring secure communications. A more secure solution would likely be necessary.

Thank you for the opportunity to appear before you today. I now look forward to answering your questions.

● (1755)

[*English*]

The Chair: Thank you very much.

We're going to start our first round of questioning with six minutes for Mr. Brassard.

Mr. John Brassard (Barrie—Innisfil, CPC): Thank you, Madam Chair; and thank you to all our witnesses for being here today. We're certainly talking about the important subject, or subjects, for that matter, of rural connectivity and privacy.

Mr. Turcotte, first, thank you for your service to our country. I know you have an extended military career and we appreciate that.

My question is in respect to the fact that Canada is a G7 country. On the issue of cybersecurity, whether it's hostile foreign power or non-state actors attempting to infiltrate these types of feeds through the mechanisms we're using, such as Zoom or others, how susceptible is Canada to the potential of cyber-attack or these non-state actors using this as a platform, as Parliament sits publicly, to attack or send a message, political, social or otherwise?

[*Translation*]

Mr. Martyn Turcotte: Madam Chair, I want to thank the member for his question.

First, I think that the people at the Communications Security Establishment of Canada would be in a better position to answer that type of question and provide more details.

Now, regarding the tools used in a virtual Parliament, it's always necessary to make a list of needs and to then see which tools would be the most suitable. As I said, each available tool provides different features and different levels of security. You can see quite clearly that there's no such thing as zero risk from a technological standpoint. An assessment of the acceptable risk must be conducted.

[*English*]

Mr. John Brassard: There is a range of organizations, from the German foreign ministry to the United States Senate, to the Government of Taiwan, to the New York City school system, that have refused to use Zoom. SpaceX's Elon Musk has refused to use Zoom.

What are they on to, and what are we missing as a result?

[*Translation*]

Mr. Martyn Turcotte: As I said, it's extremely important to make a list of needs. I'm not an expert in parliamentary procedures. Each country and each parliament has its own procedures. That said, during this COVID-19 crisis, those procedures will be amended and adjusted according to the situation. This will create new needs, which will be linked to technology needs.

To establish a virtual Parliament, I propose that the committee look at three components: the technological component, the human component and the procedural component. By placing these three components in a Venn diagram, if you will, you can determine what you need to consider to make the best decisions.

What would be applicable in Canada probably wouldn't be applicable in another parliament.

Mr. John Brassard: Thank you, Mr. Turcotte.

[*English*]

I also found it interesting that you mentioned that we were to examine this carefully, yet we've been given, effectively, five meetings to do so. Thus, it's almost impossible to go through all the scenarios and all the plausible problems from a security standpoint that it might cause.

My next question is to Ms. Qaqqaq. We know, for example, that only 40% of the rural part of our country is covered by broadband.

I will correct something that Ms. Ashton said. Actually, the opposition House leader, Candice Bergen, a Manitoba MP, was at the March 24 session of Parliament.

Ms. Qaqqaq, do you find your parliamentary privilege, your ability to represent your constituents, being jeopardized because of the ineffectiveness of rural broadband in the part of the country in which you live?

● (1800)

Ms. Mumilaaq Qaqqaq: I feel that anybody in any position in the territories is at a disadvantage if their job relies on Internet services. For example, when you renew or get your driver's licence or ID, that information needs to be sent down here to Ottawa, and then sent back into the territories, because we don't have the Internet capacity to process that. People wait months. My mother waited for over a year to get hers.

As a member of Parliament...100%. My communication is mostly on social media. If I want people to be able to have access to emails, to interact with my constituents and hear the much-needed issues and challenges my riding is facing, definitely the Internet is a huge barrier for me to be able to do that and for my constituents to be able to access space and information from me and my office.

The Chair: Thank you, Ms. Qaqqaq. That's all the time we have.

Mr. Gerretsen.

Mr. Mark Gerretsen (Kingston and the Islands, Lib.): Thank you very much, Madam Chair.

Ms. Qaqqaq, just to follow up where Mr. Brassard left off, and his question about whether you felt your parliamentary privilege had been impugned or impacted, you said 100%. Just for the record, you have never raised a question of privilege that has been addressed by the chair or the Speaker. Is that correct?

Ms. Mumilaaq Qaqqaq: I have not, but we have also never been in a global pandemic.

Mr. Mark Gerretsen: Fair enough. I just wanted to make sure that's on the record.

Mr. Leuprecht, welcome back.

For those who don't know, Mr. Leuprecht was one of my profs at Queen's University, and the only prof to ever not grant me an extension on an essay when I asked for it. If he's a little tough on me today, you'll know why.

You made a really interesting point. You said you are more concerned about how we use technology. There was a really interesting analogy for this in our first virtual session of Parliament yesterday. At the beginning of the meeting, my Zoom program had 13 pages of thumbnail photos, including one page of people who had muted their video. By about 20 minutes into it, that number had grown to five or six pages of people who had turned off their video.

What do you recommend in terms of establishing certain guidelines or best practices to make sure that people are using technology and participating properly? I think it opens the door to potential problems, which I think is what you were getting at.

Dr. Christian Leuprecht: This is an opportunity for all parliamentarians to realize—which those of us who have worked on cyber for years have been trying to push on members in Ottawa—that cyber is not just one policy domain among a series of others, and that cyber touches every aspect of our lives today. Fundamentally, we need to have a conversation about the fact that, in a democracy, human beings should not be at the service of technology. Technology needs to be at the service of human beings. The issues you just laid out demonstrate to us that we haven't thought systematically enough at the micro, meso and macro levels about how we make sure, in Canada and in a democracy, that is the case.

Mr. Mark Gerretsen: Do you think it's necessary to establish certain guidelines and principles of engagement because we should assume they're going to be different from what happens in person?

Dr. Christian Leuprecht: We are building the plane while flying it, and we especially want to be prepared for these types of eventualities. We should be having this conversation, but it is suboptimal to try to figure out what those procedures look like as we're trying to navigate the crisis and the emergency. This means that we need to have a much broader conversation about the continuity of constitutional government, so that we can be much better prepared.

You are absolutely right, we need proper procedures, and we need to learn from necessity to have a much more robust posture as a government and as Parliament, to be able to weather these types of storms.

● (1805)

Mr. Mark Gerretsen: Okay.

Ms. Bernier, I think a couple of you had talked about the fact that you're not concerned about security as it relates to public meetings. Basically, we should be encouraging people to get involved in the democratic process; therefore, there shouldn't be a concern as to the security around it. Mr. Brassard touched on something, and I'll pick up on that. I don't think the security aspect of it is just about in camera versus public. It can also be about people taking a meeting hostage. Say, for example, a very important public meeting was going to take place and a hacker got in and crashed the system and Parliament couldn't function properly as a result of that.

Would you agree that is equally concerning, or maybe not equally, but that's something that should be of concern as well?

Ms. Chantal Bernier: Indeed, there have been media reports about that. We definitely need to contend with that.

Perhaps the best way to explain my approach is to explain to you how I've come to it.

I have spent 27 years as a senior public servant, including at the highest levels. Therefore, I have been able to assess the remarkable quality of cybersecurity in government, which is why I'm quite confident that you do have the instruments and the expertise that you need. The point is to apply it in a segmented way, which means protecting information that must be protected, and protecting meetings that must be protected. Obviously, a cabinet meeting and a debate in the House of Commons do not call for the same type of security measures.

Mr. Mark Gerretsen: Okay, I understand that better. Thank you.

To both of my NDP colleagues who are joining us today, the issue of Internet connectivity is coming up. This committee is tasked with looking at a virtual Parliament right now, and one of the issues we need to look at is Internet connectivity obviously, not for entire regions but rather to make sure that every MP has the same access to the Internet.

Therefore, would it be safe to say in that context—maybe Ms. Ashton you'll want to pick up on this—provided that all MPs have the same access, it would be fair? It might cost more, but it also costs a lot more for you to travel to Ottawa than it does for me, because I'm only a two-hour drive away. Is the issue here making sure that everybody has the same level of access, and if that could be provided by, for example, satellite Internet, then we would accomplish having the same access for the purpose of a virtual Parliament?

The Chair: Mr. Gerretsen, I allowed you to get your question in, but perhaps our witnesses can answer it another time.

Next we have Madam Normandin.

[*Translation*]

Ms. Christine Normandin (Saint-Jean, BQ): First, I want to ask a question that concerns several witnesses. We're talking about a virtual Parliament, but my question pertains to another issue.

One key tool to ensure accountability, especially for the opposition, is the opportunity to hold a caucus and to talk privately. There are even rooms where the waves are blocked and where information can't get through.

Has this issue been sidestepped to some extent in favour of the virtual Parliament issue? From the start, should Parliament, including the opposition parties, have received more support to ensure the confidentiality of caucus discussions? The parties don't work with the same platforms, for example.

● (1810)

Ms. Chantal Bernier: To whom are you addressing your question, Ms. Normandin?

Ms. Christine Normandin: As I said at the start of my remarks, my question is for all the witnesses, or for those who want to respond. It concerns several issues, such as security, the importance of accountability and information protection.

I see that three witnesses want to respond.

[*English*]

The Chair: Can we have Madame Bernier first, and then Ms. Ashton? We'll carry on from there.

[*Translation*]

Ms. Chantal Bernier: Ms. Normandin, you gave a specific example of the segmentation that Mr. Turcotte and I talked about.

Not all information and debates are protected. In each segment, when you share protected information or when you want to keep a debate confidential, you must determine, with the government's cybersecurity experts, how much security you need based on the confidentiality of the debate.

Ms. Niki Ashton: Thank you for your question.

We all agree that the technicians in Parliament, the people who are helping us work virtually, are doing their best. However, we must focus on some of what we've just learned, particularly with regard to security in caucus meetings. It would be nice to have more support in this area. Yesterday, I tried to set up a meeting with colleagues on Zoom, but I noticed that the system still wasn't very flexible.

We should also look to other governments that have been doing this virtual work for some time. We must be prepared to learn from others to do the best possible job. However, we must also ensure that Parliament's work, meaning the public work, is carried out as soon as possible.

Dr. Christian Leuprecht: I want to say two things.

[*English*]

When you talk about cybersecurity, there's always a trade-off between convenience and security. The more security you want, the more inconvenient it will be for people to engage at that level. It is unlikely that we will be able to convince parliamentarians to engage in the sort of behaviour that, for instance, our defence members and our members of the intelligence community engage in for the purpose of protecting their communications. It is also a function of the networks. We simply do not have the secure networks in terms of, for instance, the level II exposed routers and purpose-built networks of the intelligence and defence communities for parliamentarians.

The challenge with a virtual Parliament is that there will be insecurity when caucus meets. Caucus will have to meet on the assumption that the information in caucus is compromised. With the conditions that we have, we cannot provide assurance that it is not. This is part of the challenge of holding a virtual Parliament. I see no way, at least in the short term, of building out a secure network and changing the behaviour of parliamentarians to the point where we can provide the level of assurance that the secure components of government have today with regard to the data protection that would be necessary for that assurance in caucus meetings.

● (1815)

The Chair: Thank you. That's all the time we have.

Ms. Blaney, please.

Ms. Rachel Blaney (North Island—Powell River, NDP): Thank you to all of the presenters today. I appreciated that information.

I would like my first question to go to Ms. Bernier and Mr. Turcotte.

One of the challenges, as we look at a virtual Parliament, is making sure that we're following the appropriate personal information protection acts. We know that forum selection clauses are pretty standard in online service contracts, but we do have a legal precedent from the Supreme Court of Canada that B.C.'s privacy laws—I'm a member of Parliament from B.C.—merit waiving forum selection clauses because they're much more stringent than other areas.

If issues arise in an online House of Commons sitting, what laws do you think would apply to the case?

Ms. Chantal Bernier: The Privacy Act, but then there is a legal void in relation to the political parties. The Privacy Act applies to all federal institutions, but the information held by political parties is not covered by the Privacy Act.

Let's therefore put your scenario in the situations where personal information would be discussed or shared in, let's say, a confidential debate. It would never be shared in a public debate unless the information is no longer protected, because, for example, it is already in the public domain. If it is exchanged in a confidential debate, it must be protected to that level of sensitivity that personal information requires. Should there be, let's say, an accidental disclosure, it would be the Privacy Act that would govern the consequences, so the obligations applicable would most likely be the Privacy Act.

Ms. Rachel Blaney: Thank you.

My other question is for my fellow MP Mumilaaq Qaqqaq.

Thank you so much for being here. I know that you had to make a very hard decision to stay in Ottawa to really be part of protecting your own community back home, but you also made it very clear that even if you were sitting in your constituency office in your riding, you are not sure that you would be able to access any committees or any virtual Parliaments. I just want to clarify that this is in fact the case.

Ms. Mumilaaq Qaqqaq: Definitely, and with my riding being the largest, I have 25 isolated communities. The capital, Iqaluit, has more services and might be a little more accessible, but as for my hometown of Baker Lake, I couldn't confidently say that. Also, even in Iqaluit, there's nowhere in the territory as of right now where I could confidently say that I would be able to participate in a virtual Parliament.

Ms. Rachel Blaney: Thank you so much. That's very helpful. As we discuss this, I think one of the issues is that a parliamentarian in this circumstance should be able to participate in their office but also in their home.

Ms. Niki Ashton, thank you again for being here today. One of the things you talked about is the need to have good regional representation, especially in a situation like this. I am from a more rural and remote community, and the challenges I'm faced with are very particular to my region. If that voice weren't heard over the long term in Ottawa, I would be very concerned.

Could you talk about the need to have that regional exposure?

Ms. Niki Ashton: Absolutely, and there's an irony, in that it's regions like ours that have some of the most vulnerable communities in the country and also some of the worst access to Internet in terms of the ability of people to live their daily lives, whether it's telehealth, accessing government services or, right now during the crisis, for kids doing their school work, or whether it's our work as members of Parliament.

We have to ensure, much like we do in normal times, that there is fair regional representation. We do that in terms of our budgets and within our parties, but let's be clear that in this time of crisis it's critical that we see a virtual Parliament as the only way we can ensure regional access.

If I could, for just one moment, I'll respond to the earlier comment by a Liberal colleague that here we are, asking about Internet for everybody. I am proud to talk about the need—the desperate need—for equal access to Internet for everybody. To be honest, I think it's very elitist that we as members of Parliament just talk about what we as individuals need, when in fact the barriers we face are a reflection of the barriers that our constituents, our neighbours and our families face in our regions.

I don't think it's out of the ordinary at all, or out of the realm of possibility at all, for a country as wealthy as Canada to invest in the infrastructure needed now for there to be equal access to Internet for all. This crisis is a wake-up call. Let's step up in this moment in time and make this possible for everybody, including MPs.

● (1820)

The Chair: Thank you. That's all the time we have.

Next is the five-minute round. We have very little time. We're going to try to get through the five-minute round.

Mr. Tochor, please.

Mr. Corey Tochor (Saskatoon—University, CPC): Thank you to all the presenters. I'll go quickly to Ms. Bernier.

If I heard you correctly, you would be comfortable having an in camera session right now with the current technology that we are utilizing in Canada.

Ms. Chantal Bernier: I would urge you to get a guarantee from the IT experts of the House of Commons that proceeding virtually in camera is secure.

Mr. Corey Tochor: Would you say that confidence has grown? Is it fair to say that two years ago you wouldn't have been as comfortable, but as technology has improved, you have become more comfortable?

Ms. Chantal Bernier: You're quite correct, because through experience, we see the risks and, therefore, develop more and more safeguards.

Mr. Corey Tochor: Thank you.

Mr. Leuprecht, I have a couple of questions for you.

This has been really eye-opening. The more we talk about this, the more I have real concerns about what this could possibly do to our democracy and our stature in the world.

Things are changing in terms of the next frontier, what we face and bad actors around the world. In the past the front lines were a lot different from today's. Is it fair to say that cybersecurity, cyber-attacks or cyber-influence of bad actors in our elections, our economy, you name it, is the next frontier? Is that a fair statement? Is that what we should be watching for?

Dr. Christian Leuprecht: If I may, I would encourage the member to read the report by the Cyberspace Solarium Commission that was released by the bipartisan U.S. congressional commission in February, which is very thorough on all the challenges that the cyber domain poses for democracy.

While we're having very technical conversations about whether a caucus is secure and whether conversations are secure, think about the adversarial intent and it is relatively straightforward. One is to sow discord in our democratic societies by polarizing conversations. The other is to show that democracy is chaotic and dysfunctional in order to hold up authoritarian systems. In a virtual Parliament, we also have the opportunity to demonstrate that democracy does function and is resilient in times of crisis, in times of emergency, because people in Russia and China can stream the Parliament as much as we can in Canada.

I think we need to be much more broadly aware of the broader objectives of our adversary over the tactical sort of dimensions of “can the adversary extract particular aspects of data”, because the adversary every day is trying to discredit democracy and sow discord.

● (1825)

Mr. Corey Tochor: Of those bad actors I can only imagine them hearing, be it government or opposition.... Probably government is where they could hear the juiciest details—what was being considered or a debate within caucus maybe. If the federal government had virtual caucus meetings—and I'm assuming they do—would that be one place for a bad actor in the world to learn juicier things and use them for economic reasons, or to destabilize? Would that be one of the juicier ways for them to hack into our Parliament?

Dr. Christian Leuprecht: One of the concerns about data being routed through servers in adversarial countries is that it opens up that data to greater vulnerability, for instance, the technology, the data assurance component. Really, it is about being able to discredit parliaments, the political executive and the way we function.

I actually think that demonstrating—with some reservations about what is discussed—the ability to continue to meet as a Parliament sends the strong message that I think we have not sent sufficiently enough, which is that democracies are actually more resilient than authoritarian systems. What is the answer to these adversarial actors to convince both the adversarial actors and Canadians that democracy is where they should be placing their faith, rather than with authoritarian systems? Parliament is the answer to that question.

Mr. Corey Tochor: Along those lines, as technology changes and improves—and this is why I asked Ms. Bernier whether she would feel more comfortable with that statement today than two years ago—so will the other bad actors in the world. Things are never static. They're going to find new and unfortunate ways.... If you think about the last 10 years, bad actors have influenced other world elections with emails, and how safe did we all think emails were, depending on the server and all that comes with that? It'll be the next step. There are additional steps we can take to make it secure, but similar to anyone who builds a fence to keep people out, people will just find taller ladders to climb the fence.

The Chair: Thank you, Mr. Tocher. I wanted to allow you time to finish your thought, and I have been trying to allow you to finish, but can you wrap it up?

Mr. Corey Tochor: Generally, if you were looking at technology to be the solution out there, along those lines, how long would it take to develop something? You talked about having separate servers and separate dedicated lines for parliamentarians. Are we talking two weeks, two months or two years to get it somewhere where you would be comfortable?

The Chair: That's all the time we have. Maybe we can get that answer another time, but I think Mr. Leuprecht was able to hear your question, at least.

Next we have Madam Petitpas Taylor.

Hon. Ginette Petitpas Taylor (Moncton—Riverview—Dieppe, Lib.): Thank you, Madam Chair.

I would like to take the opportunity as well to thank our witnesses for being with us this evening. It's always great to receive your feedback and your insight regarding this very important topic that we're studying.

As we all know, Canadians, including parliamentarians, are really trying hard to follow public health measures by staying home and working remotely. As we've heard this evening, many of us are using different platforms and different tools, and it's been quite successful for the most part, but we are also hearing concerns about cybersecurity. I know that on a daily basis we hear the words “threats” and “vulnerabilities”, and we've heard that many times this evening.

My question would probably be for Madame Bernier and perhaps Monsieur Turcotte.

What questions do you think we need to ask ourselves to ensure that we're respecting privacy concerns and security concerns in the virtual meeting part of it?

Madame Bernier, you also spoke about working remotely, and that really piqued my curiosity. I'm wondering if you would be able to elaborate a bit on that as well, as to what we should be doing and asking ourselves.

Ms. Chantal Bernier: Exactly, and as you have heard me say, I encourage you, first of all, to have a conversation with your staff. What is each of them doing to ensure that they protect information security in the context of their home? There are very specific ways to protect it. I gave you some. They are based on the major risks that we have seen through years of seeing issues. We've seen laptops lost. We have seen files left on a bus. I'm speaking of what I've seen in my five and a half years at the Office of the Privacy Commissioner of Canada, and now five and half years as external counsel.

I can tell you that there is a lot of very good, practical literature out there that really states, “These are the risks on the basis of what we've seen most often, and these are the ways to mitigate the risk.” I would encourage you to look at that very helpful literature.

● (1830)

[*Translation*]

Hon. Ginette Petitpas Taylor: Thank you, Ms. Bernier.

[*English*]

I don't know if Monsieur Turcotte wants to—

Mr. Martyn Turcotte: I'm going to echo what Madame Bernier just mentioned, but also from a technological point of view, it is important, I think, that most of the systems, if they are hosted, be self-hosted or in-house, within the organization. That's going to increase.... It doesn't mean that it's necessarily going to be perfect, but at least it's going to increase the security aspect of it, as you have full control of the infrastructure. That's one part.

The other part is in terms of mitigation. It was mentioned previously that guidelines and procedures need to be adapted. Cybersecurity is not necessarily just technology. It can be caused by humans, so having proper guidelines and procedures in place is also going to help. People need to understand their environment, so that's going to come with time and practice. The different settings and different functions that are available within the different tools you are going to use are also different types of measures or safeguards in place.

Hon. Ginette Petitpas Taylor: Thank you.

This is perhaps my last question. How would you suggest we stay current on the cyber-threat landscape, on what we're facing right now?

Perhaps Madame Bernier, Monsieur Turcotte and also Monsieur Leuprecht could respond.

Ms. Chantal Bernier: The challenge is that every day, almost every minute, one.... Ian Kerr, a professor at the University of Ottawa, who passed away last summer, sadly, and who was truly a great thinker on these subjects, used to say that when the technology is current, it is already out of date. I smiled when I heard your question, because you're referring to my everyday challenge. I constantly have to learn, because it's changing so fast.

What I would tell you is that there is a shortcut, and the shortcut is to make sure that you have a cybersecurity expert at the ready and that you have the right questions, so that what you have, then, is a good framework of what your risks are. If you know that, then you may not have the answers but you have the right questions.

You put it to them, and they will, as Monsieur Turcotte was saying earlier on, align the safeguards to the risks that you have identified.

The Chair: Okay. That's all the time we have. Thank you so much.

Next up for questioning is Mr. Duncan.

You have five minutes.

Mr. Eric Duncan (Stormont—Dundas—South Glengarry, CPC): Thank you very much, Madam Chair. I have a couple of questions, maybe as a bit of background.

Ms. Qaqqaq, I can relate to you about Internet connectivity, but probably not on the same scale that you have or in terms of the challenges you have in Nunavut. At our committee meeting last week, I was on a passionate rant to my colleagues and felt like I had their support about halfway through, when all of a sudden I was cut off and had to reconvene, right in the middle of a House of Commons committee.

One of the questions I have about connectivity when we talk about procedures and all that—and maybe Ms. Ashton can speak about this as well—is that it's important for us to understand time frames, not necessarily just for ourselves as members who may have challenges but for provincial colleagues or municipal elected officials and some of those essential services.

A fix for this, for having quality Internet access in your riding accessible to you, is not something that's going to take a couple of weeks. We lack a lot of infrastructure. Can you give some details from your community on how far we really need to go to get that parity, whether it's for you individually or members of your community in your hometown?

● (1835)

Ms. Mumilaaq Qaqqaq: Yes. Thank you for that.

To go back to what Ms. Ashton was saying, this is all so connected and intertwined with everything else. The hydro-fibre link I mentioned is also an opportunity to have a road that goes from Manitoba into the territory to a select number of communities. They're looking at similar projects over in the west, in the Kitikmeot region. In order for us to start talking about other options, we also need to be talking about things such as housing, infrastructure and accessibility to transportation.

All of these things are impacted by the lack of services. We need them in order to really increase the services, really make an investment, really make a push and really see change for the opportunity for connectivity.

Mr. Eric Duncan: Timeline-wise, you would say realistically that if we had these plans and dollars announced tomorrow, it would be months, if not maybe years, to get those communities physically connected with the fibre and what's needed.

Ms. Mumilaaq Qaqqaq: I would argue that. I think we move as fast as the federal government allows us to. We saw, for example, that when the distant early warning system was put in place, the DEW line sites across the north, it took less than two years, I think.

When we hear how things are going to take years and years, that's not true. It's only because we don't have the funding and we don't have the services. As a people, we're not treated as a priority.

I think you definitely have a fair point, though. We hear that it takes a lot of time. Realistically, it doesn't need to, but this is where we're at.

Mr. Eric Duncan: Ms. Ashton.

Ms. Niki Ashton: Thank you for your question.

Just in reiterating some of what my colleague Ms. Qaqqaq said, I think what's needed here is political will. We've seen some unprecedented investment from the federal government in recent weeks to deal with the crisis that we have in front of us right now. As I pointed out in my presentation, this crisis sheds a very bright and unflattering light on the digital divide that we have. This is deeply linked to access to health care services, access to government services and access to fundamental education.

We can do this. We have the ability to do this. I appreciate your point that we're not the only representatives who are in the same bind. Three of my provincial colleagues also live north of the travel restriction here and should not be travelling to the south, if it can be avoided, to attend the legislative assembly.

Again, though, this is a question of access to an essential service, not just for us as MPs but also, very importantly, for the citizens we represent.

Mr. Eric Duncan: [*Technical difficulty—Editor*] health care, education, and the list goes on, as you both mentioned. Thank you for your comments.

Dr. Leuprecht, we've met before, through the Eastern Ontario Wardens' Caucus. You had done a great report on policing sustainability.

For my first question I wanted to ask you maybe what you gave Mr. Gerretsen in the class you had with him. However, I'll pass on that and ask you to build on your comments about the parliamentary aspect. I respect what you say when you note that Parliament is open, transparent and on TV, in terms of the security risks there. My concern goes more to what Madam Normandin of the Bloc talked about, the caucus aspects and some of those in camera and behind the scenes stuff that are an essential part of seeing that public face of Parliament. I worry about some of those security aspects. I liked your line about building the plane while flying it, and agree that technology may not be the challenge as much as the human dynamic.

We have Zoom, for example, and we've been rolling these processes out. Do you not think that might be a human issue and not a best practice, at times? Yes, we want to get here quickly, but when you talk about the protocols, the connectivity and the devices, and those questions that you want to ask in a contract you would have with a company, do you not agree that perhaps as humans right now, who are rushing to do this, these might not be best steps, or maybe there's a higher risk of having the challenges of hacking or accessing our software outside of these programs?

Dr. Christian Leuprecht: There's—

The Chair: That's all the time we have. I'm so sorry.

Mr. Eric Duncan: Sorry.

The Chair: At least you got your question on the record. That was a little bit over time—

Mr. Eric Duncan: My apologies.

The Chair: —but I don't like to cut people off in mid-sentence.

Next up we have Mr. Alghabra. This is the last questioner for the five-minute round, and then we will switch panels.

● (1840)

Hon. Omar Alghabra (Mississauga Centre, Lib.): Good evening, Madam Chair.

I want to thank all our experts for being with us today. As I listened, I heard a lot of important questions, obviously, whether it be about accessibility to high-speed Internet or privacy concerns. Those are important public policy issues. What we're dealing with today is an exceptional and, to use a phrase that has been repeatedly used, unprecedented situation. Almost 25% of our economy has been shut down. Millions of Canadians have been asked to stay away from their jobs and stay at home. Obviously, those are extremely exceptional circumstances, and we are asking for sacrifices. I think the challenge that this committee is tasked with is that, given this context that we're in, given that we're....

In theory, I think, if you asked anybody if tomorrow we should shut down a quarter of economy, nobody would say that would be a smart thing to do or a reasonable thing to do, but we are doing it for public health reasons. We are following the advice of public health officials.

Given the situation we are dealing with, which we know is not an ideal situation, what areas or what questions should we be focusing on, given the fact that we must find at least some form of virtuality for our Parliament?

The Chair: Who's the question for?

Hon. Omar Alghabra: Mr. Leuprecht.

Dr. Christian Leuprecht: I would say that Parliament needs to prepare for whether this is a blizzard or whether we are facing a snowstorm. If we're in a prolonged snowstorm, it will require a very active engagement from Parliament with the political executive.

We also need to become much better at anticipating low-probability, high-impact events. Part of the reason we haven't been able to do that is that we haven't had an adequate strategic assessment capability within the Government of Canada for almost 30 years. These types of what you might call “black swans”, even though this is not one of them, necessitate us to have a much more robust foresight capacity of anticipating the challenges that we face and what the best arrangements are in a democracy—for instance, what should a state handle or what should the private sector handle—because I think we can't go through this again in terms of the amounts of money we are currently paying out.

Ms. Chantal Bernier: If I may, I would like to answer this question by reframing it. I think it's very important that you frame the challenge properly. It is not a privacy challenge; it is a cybersecurity challenge. It is why, for example, earlier on I heard Monsieur Turcotte refer you to the Communications Security Establishment.

You hardly ever share personal information. Privacy applies only to personal information. The broad challenge you have is one of cybersecurity, and therefore, like Monsieur Turcotte earlier on, I encourage you to seek the advice of Communications Security Establishment officials.

Hon. Omar Alghabra: Ms. Bernier, earlier you said that we should ask 100% guarantee from our IT officials. You and I know, I think, that it's almost impossible. What do you propose we should be asking for?

Ms. Chantal Bernier: First of all, you may have noticed I did not use “100%”. I said “guarantee”, but you said “100%”.

Hon. Omar Alghabra: Okay. Sorry, those are my words, but it's the same point.

Ms. Chantal Bernier: As a lawyer, I would never say “100%”.

Hon. Omar Alghabra: I stand corrected.

Ms. Chantal Bernier: That being said, my point is that to frame the challenge properly, meaning to frame it as a cybersecurity challenge, you will bring to the debate or to the discussion the information that is truly relevant and that is truly for your security experts in government.

● (1845)

The Chair: Okay. Thank you.

I'd like to thank all the witnesses for this first panel of today's meeting. You were all fantastic. Thank you for taking time out to contribute to our study. We've all learned a lot.

Now we will suspend for five minutes to set up for the next panel. Please be back at 6:50 p.m.

● (1845)

(Pause)

● (1850)

The Chair: Welcome back.

Can everyone click on their screen in the top right-hand corner to ensure that they are on gallery view? With this view you should be able to see all participants in a grid view. For those of you who are just joining us, before speaking, please wait until you're recognized by name. When you are ready to speak, you can either click on the microphone icon to activate your mike or hold down the space bar of your computer while you are speaking. When you release the space bar, your mike will mute itself, just like a walkie-talkie.

I'll remind you that all comments should be addressed through the chair. Please speak slowly and clearly. When you are not speaking, your mike should be on mute. The use of a headset is strongly encouraged.

I would now like to welcome our second panel of witnesses. We would like to hear introductory statements, first from Cristine de Clercy, associate professor in the department of political science at Western University.

Prof. Cristine de Clercy (Associate Professor, Department of Political Science, The University of Western Ontario, As an Individual): Good evening, Madam Chair and committee members.

I had intended to speak a bit in French, but given the time and the technical issues, I think I will just continue in English for the translators' ease.

Thank you for your invitation. I understand that in this panel session the committee is focusing on possible video conferencing platforms and their feasibility as it relates to establishing a virtual Parliament.

In terms of the feasibility of the technology, I expect others on this panel will discuss virtual and interactive teleconferencing in light of the capacities of different mediated platforms, albeit with some inherent limitations, security considerations and the risk of malfunction.

In terms of the feasibility of the House's capacity to amend its internal rules to facilitate members' virtual presence in lieu of their physical presence, it is clear that this can be achieved constitutionally. From J.G. Bourinot, writing in 1901, to David E. Smith, writing in 2017, in our system “legislative bodies alone are masters of their proceedings”.

As someone who studies government in Canada, my interpretation of feasibility today revolves around what sort of costs and benefits the adoption of virtual legislative meetings implies for democracy within Canada and beyond the walls of the House of Commons, so I engage this question: Is virtual assembly democratically feasible? Below are five points that may be helpful to you in your deliberations.

First, technology is intrinsically disruptive. The first taxi drivers to use cellphones to plot their courses could not imagine how this technology would alter their industry within a very short time. Plus, the law of unintended consequences warns us that intervention in complex systems tends to produce unanticipated consequences. Taken together, technology plus systemic intervention equals deep change marked by unpredictable outcomes. We cannot know the consequences of such change, but they will not all be positive for our democracy.

Second, the Canadian Parliament is unique. It is sui generis. We have a complex, diverse, finely balanced political system. In the rush to address the pandemic, it is tempting to examine how other parliamentary systems are moving towards virtual sessions, but it is a profound mistake to simply assume that what works in other systems necessarily will work the same way here. Because technology is disruptive, we need to carefully study technological adoptions and adaptations before asserting that we can estimate the effects of such change. In the history of legislatures to this point, no advanced democratic legislature deliberates and votes virtually as a method of normal business. Especially because of our complexity, Canada should not be among the first to do so.

Third, the state of democracy in Canada is not static. It has changed and evolved and continues to do so. It is dynamic and responsive to the factors and pressures that bear upon it. This is to say that the change can diminish it, as well as enhance it. Indeed, the quality of democracy can be easily damaged and insulted, as we have seen recently in some of the world's leading democracies. Any diminution in the legislature's task of holding the executive to account, or the media's key role, lessens democracy.

Fourth, considering a move to virtual House of Commons sessions and committee meetings uncovers many complex issues. Of these, one of the more perturbing concerns the deliberative function. As Valere Gaspard and I have written elsewhere, “The opportunities for formal and informal exchanges during debate, in committee work, and at work-related social activities provide crucial interactions among the members. These interactions allow MPs to be exposed to different ideas and perspectives. Such encounters are a key part of our democratic politics.... By reducing parliamentary debate, interaction and exchange to the click of a button, we risk losing what makes our democracy work.” Smith observes, “deliberation is more than an aggregation of individual constituency demands”. One of the challenges in the move to virtual assembly is to ensure that e-deliberation is more than just an episodic, half-hearted online opinion poll.

● (1855)

Fifth, other witnesses have commented on the importance of member privilege, so I will not repeat that information here. I find it difficult to accept, at this point, that virtual sittings and sessions can fully facilitate all the aspects of privilege that members enjoy when meeting in normal conditions. In particular, I expect that the privileges around political speech will be difficult to ensure and safeguard in a virtual context. The capacity of members of the House of Commons to express dissent—such as by voting against their party leadership, absenting themselves from controversial debates, challenging a ruling of the Speaker or even being removed from the House—to have that dissent understood, and to be sanctioned in known ways in accordance with the legislature's rules and the rule of law is fundamental to democracy. All manifestations of dissent demonstrate that democracy is present. It's not at all clear to me how one dissents effectively in a virtual session when those who are not speaking are literally muted. If dissent is not present and not demonstrated, then is their legislature really free?

These five points illustrate some of the costs to consider in moving to some form of a virtual assembly. Against these costs is stacked a weighty benefit: minimizing the risk of infection for MPs, staff, security, administrators, technicians and all their families. The benefit of good health is inarguable.

Therefore, the committee may well decide that meeting virtually is the best among few viable options. In this case, my view is that virtual meetings should be held very sparingly and with the understanding that these are short-term measures taken during an extraordinary period. Certainly going forward there's merit to ensuring that the House can meet virtually as a default or a backup option for future crises, and much more careful research should be undertaken as to how best to effect this. Creating this sort of institutional e-infrastructure will require a large, careful effort to fully understand the implications of such change. This period of crisis, in other words, should not serve as an accidental gateway to bringing in a permanent method of virtual assembly that is not well understood and that carries large democratic implications for Canada.

Is virtual assembly democratically feasible? Perhaps it is, but in small doses and with the intention to return to normalcy as quickly as possible.

Thank you.

● (1900)

The Chair: Thank you.

Next we have Professor Deibert from the University of Toronto, who is the director of the Citizen Lab at the Munk School of Global Affairs and Public Policy.

Mr. Ronald J. Deibert (Professor of Political Science, and Director, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, As an Individual): Thank you, Madam Chair and committee members. I'm glad to be here.

As was mentioned, I'm director of the Citizen Lab. The Citizen Lab does research on digital security issues that arise out of human rights concerns.

As much of the world moves into work-from-home rules of self-isolation, technology has become an essential lifeline; however, this sudden dependence on remote networking has opened up a whole new assortment of security and privacy risks. In light of these sudden shifts in practices, it's essential that the tools relied on for especially sensitive and high-risk communications be subjected to careful scrutiny.

In my comments, I'm going to first quickly summarize Citizen Lab's recent investigation into the security of Zoom's video conferencing application—the application we're using right now—and the company's responses to our published reports. Then I'll discuss a broader range of digital security risks that are relevant to the work-from-home routines that MPs and their staff are following. I will conclude with six recommendations.

First, with respect to our published report on Zoom, we published it on April 3 and did a follow-up on April 8. In essence, at the core of that report was that we found that Zoom did not seem to have been well designed or effectively implemented in terms of its encryption. Its public documentation made several misleading claims about its encryption protocols that did not match what we observed in our analysis. I invite committee members to take a look at that report.

We also found potential security issues with how Zoom generates and stores cryptographic information. While based in Silicon Valley, Zoom owns three companies in China, where its engineers developed the Zoom software. In some of our tests, our researchers observed encryption keys being distributed through Zoom servers in China, even when all meeting participants were outside of China. A company catering primarily to North American clients that distributes encryption keys in this way is obviously very concerning, because Zoom may be legally obligated to disclose those keys to authorities in China.

In our report published on April 3, we also discovered that there were issues with Zoom's “waiting room” feature. We didn't disclose those at the time, because we consider them very serious. We did a responsible disclosure to the company.

Now, in response to both of these reports, Zoom has taken a number of actions regarding security. It has committed to a 90-day process to identify and fix security issues, including a third party security review, enhancing their bug bounty program and preparing a transparency report. They've also committed to improving their encryption, including working towards the implementation of end-to-end encryption. They acknowledged that some Zoom users based out of China would have connected to data centres within China and indicated that they had immediately put in place measures to prevent that from happening.

They've released new versions of their platform. You can see that there are some new features, like we experienced today with waiting rooms and passwords and so forth, and they've done a very good job in terms of hiring people with credible expertise in the cybersecurity area.

While it's encouraging that Zoom has made these improvements, the sudden reliance by a very large number of people on a platform that was never designed for highly sensitive communications is symptomatic of a much larger set of problems related to work-from-home routines. It's imperative that we evaluate all the risks associated with this sudden change in routines, and not just those associated with one particular application.

Legislators working from home are connecting using devices, accounts and applications through widely differing home network setups, as are their staff. These networks may be shared with roommates and family members whose own digital security practices may vary widely. Whereas in pre-COVID times these devices were routinely brought back into the government security perimeter where sensors might detect problematic network behaviour, this is obviously no longer the case.

Generally speaking, the communications systems we rely on have rarely been designed with security in mind. Security is either routinely regarded as slowing the speed of innovation or impossible to patch backwards. The consequence is that there is a vast array of unpatched systems that leave persistent vulnerabilities for malicious actors to exploit.

● (1905)

Meanwhile, governments and criminal enterprises have dramatically increased their capabilities to exploit this ecosystem for a variety of purposes. Almost all nation states now have at least some cyber espionage capabilities. There is also a poorly regulated private market for cybersecurity that includes numerous companies that provide off-the-shelf targeted espionage and mass surveillance services. Our own research at Citizen Lab has shown that the market for commercial spyware in particular is prone to abuse and has been linked to targeted killings and the targeting of a Canadian permanent resident. These relationships may well open the door to the same tools being deployed against legislators and their staff in jurisdictions like Canada.

At the best of times, these problems present extraordinary challenges for network defenders, but now parliamentarians and their staff are at even greater risk, and threat actors are capitalizing on this new environment.

In terms of recommendations, I make six, and I'll go through these very quickly.

First, where possible, extend the digital security resources developed for the House of Commons to all Canadians. I think the IT team at the House of Commons will be severely taxed dealing with all the problems I'm describing here. Some measures have been taken already, with CSE helping out. There are ways in which the measures that CSE is undertaking to push threat indicators out to some organizations outside of the government perimeter could be done more widely, but I would urge that they be done in a transparent and accountable way.

The second recommendation is that the Government of Canada should evaluate and issue guidance on work-from-home best practices, including those for video conferencing applications. This should include recommendations for scenarios on the use of some applications for specific purposes but not others, and I assume that we'll get into that in the question and answer session. Some of that has been done already by the cyber centre, but these are dated and largely insufficient for the task at hand.

The third recommendation is to support independent research on digital security and the promotion of secure communication tools. At a time when we're depending on technological systems, there should be more high-quality, independent research that scrutinizes these systems for privacy and security risks. To assure Canadians that the networks they depend upon are secure, researchers must have the ability to dig beneath the surface of those systems, including into proprietary algorithms, without fear of reprisal. Presently, researchers can come under legal threat when they conduct this research, to the detriment of everyone's security, so we recommend that the Government of Canada pass legislation that explicitly recognizes a public interest right to engage in security research of this sort.

The fourth recommendation is to implement a vulnerability disclosure process for government agencies, including the House of Commons. These processes establish terms by which researchers can communicate the presence of vulnerabilities in organizations' systems or networks without fearing legal repercussions. I believe Canada should do this as well to mitigate vulnerabilities and make it comfortable for researchers to engage in this type of adversarial research.

The fifth recommendation is to establish a transparent and accountable vulnerabilities equities process. The Communications Security Establishment currently has a process by which it evaluates whether to conceal the presence of computer software vulnerabilities for use in its own intelligence operations or to disclose them to ensure that all devices are made secure. However, CSE is formally alone in making decisions over whether to retain or disclose a vulnerability. We therefore recommend that the Government of Canada broaden the stakeholder institutions that adjudicate whether vulnerabilities are retained or disclosed, especially in light of the enhanced risk that all government workers face when working from home. We also recommend that the Government of Canada follow international best practice and release a full vulnerabilities equities process policy, so that residents of Canada can rest assured that CSE and their government will not retain vulnerabilities that could seriously compromise the security of all Canadians.

● (1910)

My last recommendation is to support strong encryption. Given the potential for adversaries to take advantage of poorly secured devices and systems, we recommend that the Government of Canada support the availability of strong encryption so that MPs, their staff and residents of Canada can be assured that the government is not secretly weakening this life-saving and commerce-enabling technology to the detriment of all Canadians and our allies.

Thank you very much.

The Chair: Thank you, Professor.

Next up we have the Translation Bureau. We have Mr. Ball and Ms. Laliberté. Is only one of you going to give an opening statement?

Ms. Nathalie Laliberté (Vice-President, Services to Parliament and Interpretation, Translation Bureau, Department of Public Works and Government Services): Yes. I will do it, Madam Chair.

The Chair: Okay.

[*Translation*]

Ms. Nathalie Laliberté: Madam Chair, members of the committee, good evening.

My name is Nathalie Laliberté, and I am Vice-President of Services to Parliament and Interpretation at the Translation Bureau, within the Department of Public Works and Government Services. With me today is my colleague, Matthew Ball, director of interpretation and chief interpreter.

I would like to thank you for this invitation to participate in your work concerning virtual sittings of Parliament.

The Translation Bureau is mandated to provide linguistic services for these sittings, and we are happy to share our views with the committee. I would like to specify, however, that our services do not cover technical support during the sittings.

As you know, under the Translation Bureau Act, we are responsible for providing services to both houses of Parliament and to federal departments and agencies in all matters related to the making and revising of translations from one language into another of documents, and to terminology and interpretation. We provide high-quality linguistic services in the two official languages, indigenous and foreign languages, and sign languages.

The Translation Bureau plays a vital role in implementing the Official Languages Act. This role makes the bureau a key player in communications with the public, the language of work in the public service, and the advancement of English and French in Canadian society.

Since 2017, we have followed a clear vision to guide our future as a centre of excellence in linguistic services for the Government of Canada. Under that vision, we launched major initiatives to increase quality control, modernize our business model and provide the most advanced language tools.

We expanded our capacity to provide services in indigenous languages, and we increased co-operation with the language industry in Canada. We introduced ways to better support our employees, deliver the training they need and take care of their mental health.

We revamped our recruitment processes and created partnerships to support the next generation of language professionals. For instance, we participate in the master of conference interpretation program at the University of Ottawa. We loan equipment and instructors to the university and, in return, we benefit from a pool of highly skilled new interpreters.

[*English*]

We are applying the same forward-looking approach as we adapt to the COVID-19 pandemic. Since mid-March, as you've seen, we've continued to focus on carrying out our mandate in helping Parliament meet its responsibility concerning the interpretation of proceedings and the translation of documents. That being said, we have the same issue with reduced capacity as the rest of government.

Luckily for us, translation lends itself particularly well to telework, and we've been able to maintain our services while having our translators work from home. As for interpretation, which is the focus of our discussions today, the bureau has been providing this service since 1959. Through the years, we have been successfully maintaining our services through the dedication of our outstanding employees and freelancers.

In this period of pandemic, given the technical requirements of interpretation, interpreters must continue to work on site in Parliament. However, I can assure you that their health is a top priority, and we have carefully applied expert advice to protect them.

We have added portable interpretation booths and installed partitions in existing booths so that there is some separation between interpreters who share the same booth. Interpretation booths are disinfected twice a day. We've provided interpreters with disinfectant wipes so that they can disinfect equipment before and after each assignment. We have loaned tablets to interpreters so that they can consult background information in the booth, without having to handle printed documents. We have reduced the size of teams and applied physical distancing rules to prevent contact between interpreters. We've made parking spaces available to interpreters so that they do not have to use public transit. We're taking into account the circumstances of interpreters who have young children or who must stay at home for other reasons, and we're keeping the lines of communication open with the unions.

You will ask, can an interpreter work from home? We've started to explore this possibility, but remote interpretation poses major challenges.

● (1915)

We use the term “remote interpretation” when one or more participants are not in the same location as the interpreters. In recent years, the increased popularity and accessibility of video conferencing has led to an ever-growing demand for remote interpretation. In response to this demand, the Translation Bureau began conducting its own tests and studying international best practices. However, the sudden onset of the pandemic forced us to step up our efforts, and for the last few weeks we've been actively working on this matter in collaboration with the House administration.

We have determined that certain criteria must be met in order for remote interpretation to work. These include the following: All participants must wear a headset with a microphone to ensure clear sound quality; participants must appear via video conference so that the interpreter can see their facial expressions and clearly communicate the tone of their message; participants must strictly adhere to the rules for speaking and must wait their turn to speak; a technician must be in the room with the interpreters at all times to address any technical issues; the audio feed of the interpretation consoles must have limiters or compressors to prevent acoustic shock; interpreters must be able to do sound checks with the technician and participants before each meeting begins; and, as always, participants who plan to read written statements must provide them in advance to our interpreters.

These criteria are needed to establish the optimal conditions so that interpreters can provide high-quality services in a safe environment. Abiding by these criteria will not completely eliminate the risk of interpretation service interruptions due to the technology used by remote participants, but it will greatly reduce this risk and help ensure the best possible interpretation.

The criteria on sound quality are particularly important, since sound is the cornerstone of interpretation. For example, if the sound quality is poor, an interpreter may mix up the words “symptomatic” and “asymptomatic”, which completely changes the message. Furthermore, poor sound quality puts the interpreter at risk. In the last two years, several health and safety incidents have been reported involving sound issues during teleconferences and video conferences.

Regarding the human resources required to provide interpretation at virtual sittings, the Translation Bureau will augment its team of interpreters. Variation in sound quality means that interpreters have to concentrate harder, which means they have to work shorter shifts. This means that we need to assign more interpreters per sitting. However, we will make every effort to meet this need.

[*Translation*]

Madam Chair, members of the committee, our mission is clear: we are here to serve Parliament, and we are doing our best to respond to the call. We are committed to pursuing our collaboration with the House administration and all our partners to help ensure that a virtual Parliament runs smoothly.

The Translation Bureau is proud to be able to help Parliament continue its essential work during this crisis, and we are proud to help the Government of Canada share the information Canadians need to stay healthy and up to date on what is happening in English, French, American Sign Language and Quebec Sign Language.

I would like to specifically commend our official language and sign language interpreters for the incredible work they are doing every day at the various press conferences. This crisis has shone a spotlight on their excellent work, and we are grateful for their dedication.

To close, I would like to thank the interpreters at this meeting. In addition, thank you to all the employees who work behind the scenes to make important meetings like this one possible, despite the difficult circumstances we find ourselves in. I would like to extend a special thank you to our invaluable partners at the House multimedia service and the committees directorate. I am sure you appreciate their efforts and expertise as much as I do.

Lastly, thank you, Madam Chair and members of the committee, for your attention and your interest in our services. Mr. Ball and I would be happy to answer your questions.

● (1920)

[*English*]

The Chair: Thank you, Madame Laliberté.

Our next witness is Mr. John Weigelt from Microsoft Canada. He is the national technology officer.

[*Translation*]

Mr. John Weigelt (National Technology Officer, Microsoft Canada Inc.): Thank you, Madam Chair.

I am pleased to be here today.

[*English*]

My name is John Weigelt. I'm the national technology officer for Microsoft in Canada.

I've had the privilege of working with the federal government for my over 30-year career in trustworthy computing, starting in uniform in the Royal Canadian Air Force, in the Treasury Board Secretariat as a public servant, and now as CTO at Microsoft Canada.

I'm grateful for the opportunity to appear before this esteemed committee and its members today as you discuss how technology can support the continuation of the Parliament of Canada during this unprecedented time. My remarks will focus on a thoughtful and deliberate approach to using technology to support virtual parliamentary activities, with privacy and security as the foundation.

You may ask yourself why we're focusing on security, as parliamentary proceedings are public and do not contain sensitive information. Microsoft believes that security must be the foundation of everything you do with technology, regardless of whether it's publicly available or involves sensitive material. Security protects against unwanted intrusions causing disruptions or introducing cyber-threats.

First, I'll give you some background.

Microsoft has a long history here in Canada. Since the establishment of Microsoft Canada in 1985, Microsoft's presence has grown to include 10 regional offices around the country, which employ more than 2,300 people. At our Microsoft Vancouver development centre, over 700 employees are developing products that are used around the world. Cutting-edge research on artificial intelligence is also being conducted by Ph.D.s and engineers at Microsoft Research Montreal.

These unprecedented times have forced every person in the world to adapt and dramatically change all aspects of their lives: how they work, how they learn and how they interact. We are proud to have enabled remote learning for students and educators. Virtual health visits are allowing for the delivery of health care while protecting patients and health care workers, and Microsoft technologies are empowering millions of Canadian workers in all sectors of the economy to work remotely during this COVID crisis. In fact, today over 100,000 federal public servants are now working remotely using Microsoft Teams, and this number is growing every day.

Today's technology and video conferencing capabilities are built on what we call cloud services. A cloud is information technology infrastructure upon which these virtual activities rely, and the safety and reliability of this cloud are key. Microsoft has been a longstanding partner of the Government of Canada, supporting the development of a thoughtful and deliberate approach through policy, guidance and standards for the government's adoption of cloud services. This strong partnership has enabled the rapid deployment of technology tools in response to the COVID crisis.

Our Canadian data centres in Toronto and Quebec City were the first to undergo independent audits and reviews against the government's security standard. As a result, the government certified Microsoft's services to safeguard the Government of Canada's information at the Protected B level. This is the government security classification for sensitive and personal information.

In addition, Microsoft has also worked with leading Canadian privacy experts to conduct a review of these services. We've published and shared this analysis in what is called foundational privacy impact assessments, setting a precedent across the industry. These assessments help public sector organizations of all types across the country understand how Microsoft cloud services, including video conferencing, address their privacy obligations. In addition, we're the only cloud provider that publishes all of our compliance and audit information, as well as the results of our security tests, publicly on our website.

I'm here to tell you that technology exists today to support virtual parliaments in a secure manner. Using our Microsoft Teams platform, we've been supporting parliaments in various jurisdictions. For example, the U.K. House of Lords is currently sitting remotely via Microsoft Teams, as are committees of the Quebec National Assembly. Virtual activities in these jurisdictions have been the result of close collaboration between the various Microsoft teams and the procedural and technical teams of these legislatures. This is new for everybody, and putting in place virtual parliamentary activity has required flexibility and adaptation on everyone's part. It's a mix of technology, process and people.

With over 75 million daily users worldwide, and now having exceeded 2.7 billion meeting minutes in a day, Microsoft Teams provides a robust environment for people to do their best collaborative work. It includes video conferencing and has many of the same features you've come to know with Skype and Skype for Business.

But video conferencing is only the beginning of what Microsoft Teams can do.

● (1925)

While the emphasis in this conversation has been on video conferencing capabilities, this flexible platform offers a broad set of collaboration services that we believe are useful in digitally transforming government and committee meetings. For example, it could facilitate the transfer of meeting minutes, pre-readings and written submissions. While we recognize that this is not a priority in the short term, this should be something that Parliament looks at in the future term. Microsoft Teams has the ability to support this activity in a secure way.

Further embedded in Microsoft Teams are a variety of assistive technologies to support individuals with unique accessibility requirements due to mobility, seeing or hearing challenges. We are pleased that Microsoft Teams is currently in the process of being deployed to each member of Parliament and employees of the House of Commons.

To be clear, security is at the heart of everything we do at Microsoft. We employ over 3,500 security engineers and run the Microsoft security response centre, which operates 24 hours per day, seven days per week, every day of the year. We analyze trillions of events encountered from our global footprint to keep ahead of threats. Since security is a shared responsibility that no single organization can address on its own, we have exceptionally strong connections to the government's cybersecurity team, and we work together to protect both the federal government's cyberspace and Canada's cyberspace.

While the technology does exist to support virtual Parliament, there are still privacy and security considerations despite the public nature of these meetings. For example, in the virtual space, how would you prevent unwanted disruptions by unauthorized individuals? Just imagine for a moment, if you will, that the public galleries are filled with hundreds of unruly spectators. In the physical space, the Sergeant-at-Arms and the Parliamentary Protective Service would ensure that they don't cause unwanted disruptions. How would you put in place similar safeguards in a virtual space to protect the integrity of proceedings? Solving for these security and privacy issues is a matter of correctly configuring privacy and security controls, and also making sure that you have the right security development cycle.

Similarly, individuals should have confidence that the software they deploy on devices, whether it's Windows, their Mac, their iPhone or Android, only does what they expect it to do. Recognizing this as a top priority for customers almost 20 years ago, Microsoft implemented the trustworthy computing initiative. This means that privacy and security are part of every step of the development of our products and services, and follow the privacy-by-design principles, which were invented here in Canada. This is a fundamental commitment that Microsoft makes to its customers.

Microsoft's privacy commitments, which exceed those found in Canada's privacy legislation, provide the confidence that Microsoft will never use customer data for any other purpose than providing the service.

In closing, I fully recognize the complexity of the procedural and technical work associated with examining remote options, and I applaud this committee's very important work and the work of the House of Commons. I have deep respect for the institutions of Parliament, and I am confident that the possibilities technology can offer to support your work in a virtual fashion can enable parliamentary activities to take place in a new and different way, all while maintaining the integrity of the democratic system.

It will be my pleasure to receive your questions. Thank you.

The Chair: Thank you.

Next we have Mr. Harry Moseley, global chief information officer for Zoom Video Communications.

● (1930)

Mr. Harry Moseley (Global Chief Information Officer, Zoom Video Communications, Inc.): Thank you, Madam Chair and members of the committee, for inviting Zoom to participate in this important hearing today.

I firmly believe that the role you play and your decisions on how best to proceed with Parliament in these extraordinary times are truly significant. Ensuring that the House of Commons continues to be productive and operational is more important than ever.

We at Zoom are committed to helping support your efforts and to providing any information you need in advance of your presentation to Parliament on May 15. With millions of people around the world working from home due to COVID-19, video communication companies like Zoom are playing an integral role in ensuring that businesses, hospitals, schools and, importantly, government can continue to collaborate securely and remain operational.

Zoom recognized early on that we were uniquely positioned to help in this time of need, and we felt compelled to act. We feel a tremendous responsibility to our users. In February, we committed to doing everything in our power to support those impacted by COVID-19, and that promise very much continues to date.

By way of background, I have over 40 years of technology experience, most recently as the CIO for KPMG U.S. and the CIO for Blackstone. In December 2017, I retired, and shortly afterwards Zoom invited me to join them as their global CIO. Once I met Eric Yuan, our CEO and founder, and conferred with industry veterans and my peers, I was inspired to join his elite team. Eric, who had 14 years of experience building Webex, and a team of engineers founded Zoom in the U.S. almost 10 years ago, in their mission to build a seamless and frictionless video-first communications platform based on four principles: security, reliability, functionality and cost-effectiveness for their customers.

There were several objectives, most notably the seamless and frictionless experience, intuitive ease of use, the elimination of the "meeting tax", and doing this agnostically across platforms to enable the energy of the participants to be focused on the substance and not the logistics and operations of the meeting.

Today, Zoom is the leader in modern enterprise video communications. Zoom's sole focus is providing a secure, reliable platform that works seamlessly across devices and is incredibly easy to use. We are proud of what we have accomplished with our users, from individual subscribers to the world's largest global enterprises, which is reflected in our customer satisfaction in the 90-plus percentile.

There is a reason people say, "Zoom, it just works." In light of COVID-19, usage of Zoom has ballooned in recent months. We have grown from 10 million daily meeting participants as of December 2019, to over 300 million per day in April, with incredible service reliability. We are proud to be doing our part to keep people connected and organizations working during the pandemic.

As part of this effort, we opened up the platform to new types of users, such as offering free video conferencing to primary and secondary schools around the world. To date, over 100,000 schools in 25 countries have used Zoom's free services to stay connected to their students during this pandemic. We have also served numerous government customers for years, and in the current environment, with COVID-19, our service has become more essential than ever to ensure that governments around the world can continue to function during the difficult days ahead.

For example, in the U.K., we are proud to be helping MPs fulfill their parliamentary duties. They have successfully rolled out a hybrid Parliament with a maximum of 50 lawmakers physically in the debating chamber and another 120 permitted to join via Zoom.

In Canada, we are humbled to have been selected to support the House of Commons. We have worked very closely with Soufiane Ben Moussa, the CTO of the House of Commons, to ensure that we are providing Zoom's trademark ease of use coupled with training on Zoom's leading security features, as well as technical support to meet specifications such as enabling simultaneous channels for English and French.

● (1935)

We have always been a leader in innovating at speed and scale, and are equally committed to doing that with respect to privacy and security. In its current form, Zoom unequivocally delivers a safe and secure virtual meeting environment when used with the appropriate safeguards to protect meetings. As sophisticated organizations across the globe do exhaustive security reviews of our user network and data centre layers, they continue to confidently select Zoom for complete deployment. In fact, we have seen a surge in this regard recently.

To echo the words of our CEO, our chief concern is ensuring that the safety, privacy and security of our platform is worthy of the trust our users have put in us. As such, and in light of new use cases and public attention on Zoom, we have made a number of changes across the platform. We have wasted no time in executing the 90-day plan we announced on April 1 to better identify, address and fix issues proactively. A summary of our plan, including all of the actions we committed to, can be found in the briefing materials we submitted.

A couple of examples include that we enacted a feature freeze and shifted all of our engineering resources to focus on trust, safety, security and privacy. We also launched an industry agnostic CISO council, in partnership with leading CISOs, to facilitate an ongoing dialogue regarding security and privacy best practices.

Most recently, we announced robust security enhancements with the general availability of Zoom 5.0, which, among other key features, adds support for AES-256 GCM encryption across Zoom's infrastructure. This increased level of encryption enables Zoom to provide industry-leading protection for meeting data and resistance against tampering and unauthorized access. Zoom's security features, which have previously been accessed throughout the meeting menus, are now at hosts' fingertips. They are grouped together and easily found by clicking the security icon in the meeting menu bar on the host's interface.

With regard to data routing there are several facts that I would like to share. The Zoom platform only collects information necessary to provide the service. Where all meeting participants are using the Zoom client, all meeting data—audio, video and content—is fully encrypted among all participants, and it is never encrypted until it reaches a participant's device, including its transit through our data centres. There are exceptions to this, such as a participant joining via a phone line, a cloud recording or other features—for example, streaming to YouTube without encryption being enabled.

Zoom has 17 data centres around the world, one in Toronto and one in Vancouver. We supplement our data centres with cloud providers, which, among other things, are used for authentication, cloud recordings and metrics.

We also understand there are concerns and sensitivities around data travelling to certain countries. We maintain geofencing around China specifically, ensuring that users outside of China do not have their meeting data routed through China. We are aware of recent reports suggesting that a small fraction of non-China meetings were inadvertently routed through Chinese servers. Zoom investigated this issue and has ensured that it will never happen again.

To provide additional comfort and control for our users, we recently added a feature that enables paid Zoom customers to customize which data centre regions their account can use for real-time meeting traffic. We also enhanced the Zoom administration dashboard to show additional transparency on data routing.

● (1940)

With respect to privacy, Zoom does not and has never sold user data; does not monitor meetings or their contents; and complies with all applicable privacy laws, rules and regulations in the jurisdictions within which it operates. Zoom has fully implemented compliance programs designed to meet the requirements of the Canadian data protection regulations, including the Personal Information Protection and Electronics Document Act.

The Chair: Thank you, Mr. Moseley. Our time is up.

Do you have much more to summarize?

Mr. Harry Moseley: No. I have one minute.

The Chair: Okay.

One more minute.

Mr. Harry Moseley: We know there has been a lot of media attention on Zoom due to recent new use cases as noted previously. Zoom has been recognized to have seriously stepped up to enhance its privacy and security in short order by amplifying safeguards and addressing issues quickly.

In conclusion, I can assure you that we continue to be the easiest to use and most functional platform on the market. Our commitment to security cannot be topped. This is also a continuous journey for us. Rest assured that security is and will be at the top of our list.

We are grateful to have the opportunity to speak to you this evening and to answer any questions you may have about how video conferencing companies and Zoom specifically can support the House of Commons. We think of our clients as partners. Our singular objective is your success in using our platforms securely and in a reliable fashion. I know that Zoom is well positioned to continue serving the House of Commons.

Thank you for your time and attention.

The Chair: Thank you, Mr. Moseley.

Thank you to all of our witnesses.

I think I can speak on behalf of the committee and say that this has been a very informative panel and meeting, hitting issues such as respect for Parliament, the privilege of members, bilingualism, which is very important of course, and our technological solutions, including how we can make sure that they're safe and private.

We will continue into our first round of questions with the members.

We will definitely get through the first round of six-minute questions. At that point I will ask the committee members whether we can get in a few more questions after that.

Mr. Richards, we'll start with you.

Mr. Blake Richards (Banff—Airdrie, CPC): If I can, I first have a point of order, Madam Chair.

Can you just refresh my memory? The first round of questions would mean what?

The Chair: Of course I'm willing to go as long as we're able to. I have to consult with the clerk as well.

The first round of questions is for six minutes. The Conservatives, the Liberals, the Bloc and the NDP each get one.

Mr. Blake Richards: Okay.

For the sake of managing our time, could we as a committee decide now on what we are going to do in terms of questioning before we begin?

The Chair: Absolutely.

If I may suggest, we could change it into five-minute rounds and maybe do the next round for four minutes. I think we could squeeze it in. Let me just confirm with the clerk to see what we can manage.

Mr. Blake Richards: Thanks, Madam Chair.

The Chair: I was conferring with the staff in the committee room. We do have some flexibility on their behalf. They would be able to accommodate us up to 8:30, if that is okay with the witnesses and the committee members.

That would allow us to get in the second round as well.

Yes, the witnesses have said it's okay.

Yes, Mr. Gerretsen.

Mr. Mark Gerretsen: Can we commit ourselves to that first and second round? If that ends at 8:15, then we'll end at 8:15.

Is that agreed?

The Chair: Is that okay with everyone? Yes?

All right, thank you for resolving that at the get-go.

We will start with our first questioner, Mr. Richards.

Mr. Blake Richards: Thanks, Madam Chair.

Most, if not all of my questions, will be for the Translation Bureau.

First, when we were studying the issue of indigenous languages in House proceedings in the previous Parliament—I think two or three years ago now—when the Translation Bureau came before the committee at that time, speaking about remote interpretation being tried out, the Bureau indicated the following:

> ...there are still issues that need to be addressed before we can offer this service on a regular basis. The two key issues are audio quality and bandwidths, which can be erratic, resulting in variable audio quality for interpreters and clients alike.

A lot of other witnesses at that time raised this issue as a concern as well.

I'm wondering if those issues have been resolved satisfactorily for you to be able to change your opinion at this point.

● (1945)

Ms. Nathalie Laliberté: Sound quality is the cornerstone for interpretation. When participants are remote, the sound is really dependent on the Internet connection of the participant, on whether they're using a headset and on some of the technical requirements I mentioned in my opening remarks. It's very important for the Translation Bureau that those technical requirements are met when we provide services.

When those are met, there will be less risk of a service interruption. If an interpreter cannot hear, they will not be able to interpret. We're working closely with our clients and with the House administration—it's really a team—to ensure that the technical requirements are met so that the quality of the sound is sufficient for an interpreter to be able to do his or her job.

Mr. Blake Richards: Would you say there is a chance that the quality will suffer as a result?

Ms. Nathalie Laliberté: Will the quality suffer? No, it won't because of what we ask of interpreters: if they cannot hear, they cannot interpret, so we've provided them with that at our end to protect their health and safety as well. When you hear “inaudible” or you hear that the interpreters are stopping, it's because they really cannot hear, and they won't guess, to make sure that they deliver quality service.

Mr. Blake Richards: Okay. We saw that yesterday, certainly, in the committee of the whole that sort of replaces question period. There were times when interpreters were indicating that they couldn't hear satisfactorily.

You also mentioned in your opening remarks—and I know it's in the briefs we've received from some of the associations—that there's been a need for more interpreters. Just given the fact that they aren't in the same room and the visual ability to see is not there, it's harder on them. [*Technical difficulty—Editor*] that seems to be what you've indicated as well, and I can certainly understand how that would be the case.

I wanted to get your take on this lack of visual ability to see in some cases being more difficult for interpreters. Just tell us a bit about how your team is holding up—

The Chair: I'm sorry, Mr. Richards. I'll pause your time. Could you put your headset on? There is some static that we're hearing. It's difficult for the interpreters.

Mr. Blake Richards: I'm sorry. I don't have it handy, unfortunately. That's why I'm not using it. My apologies for that. I think it was just my phone. I'll move that away.

Is that better?

The Chair: Yes, it is better. Could you be as close as possible to the screen and move your phone?

Mr. Blake Richards: Sure. Understood. I did move the phone.

Were you able to get my question or do you need me to repeat it?

Ms. Nathalie Laliberté: I was able to get your question.

Mr. Blake Richards: Okay. Thank you.

Ms. Nathalie Laliberté: Yes, when we have the interpreters interpreting remote participants, we need to increase the team's strength. Normally, on average—it varies depending on the type of assignment—an interpreter in a normal setting will do it for about six hours. With remote interpretation, it's much harder for them to do it. It increases the cognitive load, so on average they will do about four hours instead of six, and we bring in more teams of people to do the work.

In addition to that, we've added on site a coordinator who is also an interpreter and who will deal with the technical issues with the technicians and make sure that the interpreters get all of the documentation so that it's much easier for them to do their work. In summary, the interpreters do a shorter time in the booth, we have coordinators and we—

Yes?

Mr. Blake Richards: What challenges has that created, if any? Has it created challenges for the interpreters? Have there been more sick days or challenges in how they are holding up? There's obviously only a limited number of professionals who are qualified to do this work, so I wanted to see what kind of impact it has had on them.

● (1950)

Ms. Nathalie Laliberté: Thank you for raising that point.

I have to say that the conditions are difficult for the interpreters. Some interpreters have reported incidents, saying that after assignments they have headaches, earaches and fatigue. There were no incidents related to acoustic shock or injury requiring medical assistance, but it's much harder on the interpreters to do their work because the sound varies with the connections of the participants. They really have to concentrate harder.

I'm not an interpreter by trade, and I really admire the work of my team, because what they do is that they listen to the participant and then in their head they have to analyze, translate the information and put it into the other language in a flow that works, and they speak on top of that. They do all of that at the same time, so really, the cognitive load of what they have to do is extremely difficult in normal circumstances, and when it's remote, it's even harder.

Mr. Blake Richards: Okay. Thank you.

The Chair: That's about all the time we have, Mr. Richards.

Mr. Blake Richards: Okay. No problem.

Thanks, Madam Chair.

The Chair: Mr. Gerretsen.

Mr. Mark Gerretsen: Mr. Moseley, I've been dying to ask you this since we started this meeting. Is that a real or virtual background?

You're on mute.

Do you know how to use the platform?

Mr. Harry Moseley: I did some training earlier today.

Voices: Oh, oh!

Mr. Harry Moseley: Luckily...

Mr. Mark Gerretsen: I think you said it's a virtual background.

Mr. Harry Moseley: That's a virtual background. I can put up other virtual backgrounds if you want me to.

Mr. Mark Gerretsen: No, my time is limited.

My question for you is what is the minimum required Internet speed for Zoom to function properly?

Mr. Harry Moseley: That's a great question. Thank you.

Madam Chair, a great part of our technology is our technology architecture, which is radically different. When a meeting starts on Zoom, like this meeting, it's held in one of our 17 global data centres around the world. Now I would like to be clear with respect to the Canadian House of Commons: Your meetings and all of your data are all resident in Canada in two data centres, Vancouver and Toronto. None of your data is ever held outside. Saying it differently, everything for Canada's House of Commons is inside Canada and not outside.

Mr. Mark Gerretsen: And the security?

Mr. Harry Moseley: I'll come to your question. It has to be explained.

When that meeting happens, it connects to each of the end points, and we handle that network connection discretely end point by end point. We can tolerate what's called a 45% packet loss and still have a fantastic experience because we always prioritize the audio over video over content. We handle really poor networks in extraordinarily good circumstances.

Mr. Mark Gerretsen: In the earlier panel we talked a lot about Internet connectivity in rural parts of the country. We heard some numbers about people getting 8 megabytes per second here or there, and so on and so forth. Do you have an actual number for the minimum number of megabytes per second required for Zoom to work properly?

Mr. Harry Moseley: I don't, but we can certainly get that.

Mr. Mark Gerretsen: Yes, if you could.

Mr. Weigelt, do you have any information on your Microsoft Teams platform in terms of connectivity?

Mr. John Weigelt: Well, we see access to connectivity as being a challenge across Canada, and it's one of the things that's critically important for us as a company. We have our Airband project that is looking to reach out and provide connectivity options where there is no access. We're quite proud that we have 2,500 people using Teams out of Nunavut and being able to get exceptional services over a satellite link. Our key concern is around what we call “latency”. It's that delay, that lag, between the beginning and the end of a conversation. As was indicated with the other tool sets, we make sure that we prioritize the voice conversation first, and then we are able to manage across what we call “disadvantaged links”.

Mr. Mark Gerretsen: I can appreciate that you don't have an exact number either, but if we could get from both of you some kind of breakdown information on what Internet speed is required to have a decent connection....

Full disclosure, I was a computer engineer. That was my original training. I can appreciate that it's very complex and not as simple as just giving me a number like that, but if we could get some info on that, it would be great.

Madame Laliberté, you had some extremely good points about translation and how this is going to work. This committee right now is tasked, to my understanding at least, with how we can have a virtual parliament in the short term in light of COVID-19. If we were to design something that was going to last over a much longer time, I think we could really drill down to get to the core issues of what is required in terms of what you were asking. But if there were one thing or a couple of things that are really necessary to make this work in the short term, given the situation that we're in right now, what improvements could be made?

● (1955)

Ms. Nathalie Laliberté: I would say that the most important thing is that people wear a headset. We've done a lot of tests over the last few years, and even more over the last few weeks, and the quality of sound is much better when people wear their headset. This is of prime importance, though—

Mr. Mark Gerretsen: Sorry, but if we were to make one of our recommendations that headsets be mandatory, your organization would support that, obviously.

Ms. Nathalie Laliberté: Yes.

Mr. Mark Gerretsen: Is there anything else on that same theme that comes to mind, perhaps in terms of the health implications for employees? Is there anything we can do to deal with this in the short term?

You have about 30 seconds.

Ms. Nathalie Laliberté: I will send the question to Matthew Ball, the chief interpreter.

Mr. Mark Gerretsen: Could you answer that, sir?

Mr. Matthew Ball (Director, Interpretation and Chief Interpreter, Translation Bureau, Department of Public Works and Government Services): Sure. There are a few things that can significantly improve the situation for interpreters.

One that is possible for many people, but not everyone, is to have a hard-wired Ethernet connection. It's what I'm using today. It means that you're not dependent on Wi-Fi and don't have connectivity issues.

Another one that's really important and really easy for everyone is to send texts in advance. I'm sure all of the witnesses here today had prepared texts. Members of Parliament are often reading from texts. It's really helpful for the interpreters to receive those texts, especially when you plan to read them quickly, because they tell them basically what you're going to say and have the facts and figures. Interpreters are used to checking against verification, so they won't read them blindly, but they really help. Those are two of the most important things for us.

Mr. Mark Gerretsen: Perfect.

The Chair: Thank you. That's all the time we have.

Madame Normandin.

[*Translation*]

Ms. Christine Normandin: Thank you, Madam Chair.

I'd like to ask Ms. Laliberté and Mr. Ball a few questions, if I may.

You said you were in need of more interpreters right now to ensure their health and safety. Since there are more English speakers than French speakers in the House of Commons, I imagine that puts greater pressure on interpreters who work from English to French.

It was recently announced in the House of Commons that cleaning product labels would not necessarily be translated into French because doing so could be a hindrance in the context of the crisis.

Does it worry you that the usual level of institutional bilingualism can't be maintained in light of the current circumstances?

Ms. Nathalie Laliberté: Thank you for your question.

All the interpreters who work for the Translation Bureau and Parliament are accredited by the Bureau. They are accredited in their mother tongue and in what we call their B language. That means they can all interpret from one language to the other. The Bureau is accustomed to the fact that the volume of work into French is always greater than into English, so we don't foresee any capacity issues in the near or even long term, in either language. We have significant capacity in both official languages.

Ms. Christine Normandin: Very well.

In the circumstances, are more people working in their other language, in other words, going from their B language to their A language?

Ms. Nathalie Laliberté: I don't think so because we have strong capacity in both official languages. Some interpreters are quite comfortable working in either language, while others are less so, be they Translation Bureau employees or freelancers. No one is forced to work in a language they aren't comfortable in, particularly in Parliament, whose proceedings are broadcast. We've never had a problem in that regard, and we don't anticipate one in the near future.

● (2000)

Ms. Christine Normandin: I'd like to know how it works when interpreters advise you of problems they experience in their day-to-day work. How and to what extent do you receive feedback? Have you seen an increase in the number of requests, complaints and grievances?

Ms. Nathalie Laliberté: Thank you for your question.

We work closely with our interpretation teams. After every test, after every assignment, interpreters provide a report. We also work closely with the union. We meet with union representatives twice a week, and we discuss the various challenges and issues that we can work on. We manage to find solutions to most of the concerns that are brought to our attention. We've installed plexiglass in some of the interpretation booths, and earlier this week, some committee rooms were equipped with plexiglass as well. We work closely with the interpreters, and we always strive to find a way to resolve their issues. Of course, their job isn't easy given their difficult working conditions, and yet, despite all that, they show up for work every day and do an outstanding job.

Ms. Christine Normandin: Thank you very much, Ms. Laliberté.

Now I have a few practical questions for Mr. Weigelt and Mr. Moseley.

We are trying to set up a virtual Parliament, so we need to re-create some of the principles of the physical Parliament.

Do your platforms offer the capability to raise your hand, similar to a classroom? In actual Parliament, the Speaker or chair chooses who to give the floor to. How could that be re-created on your platforms? Is it possible to establish an order to identify who raised their hand first? Do your platforms have a way to keep track of time, so we knew how much time we had used and how much we had left?

[*English*]

Mr. Harry Moseley: As you can see, I raised my hand.

Sorry, I didn't address you, Madam Chair. My apologies.

The Chair: That's okay. Go ahead.

Mr. Harry Moseley: Sorry. I'm not used to these normal proceedings.

Madam Chair, you can see I raised my hand. We already have that capability built into our platform. I can lower my hand.

With respect to timing, we have a time clock that shows the duration of the meeting. If you were interested in a timing feature, for example if I have 10 minutes to speak, I could have the system it count down, that is something I would be happy to take back to our product people to see if we can get that into the platform for you.

We have a practice at Zoom of listening to our clients. If that's a feature that would be helpful for the Canadian House of Commons to use our platform, then we will evaluate that and I can come back to you by the end of this week at the latest.

Mr. John Weigelt: Within the team's platform you have the capability also to raise your hand to get the attention of the Speaker. Much like the House of Commons has provided guidance around how to best leverage video conferencing, we also recommend that the chat stream form part of that interaction, and thus the ability to then share thoughts. Sometimes people don't always watch the raise-the-hand signal.

We also have a timer to time people, or to see how much time is left in the meeting or how long people have spoken. I think those things are part of that.

When we deployed these solutions at the beginning, we deployed them in support of what we thought were generalized uses. As we built them out, we've heard from our customers, be they in the education sector or the health care sector, that they need tweaks to those particular toolsets. We've gone back to our engineers to make sure that those tweaks come in.

You saw those tweaks rolling out April 21. You'll see over the next few weeks you'll get an increasing number of features. That's the power of cloud services.

The Chair: Thank you. That's all the time we have.

Ms. Blaney, please.

● (2005)

Ms. Rachel Blaney: Thank you. I thank all the witnesses for being here today. I appreciate your testimony so much.

I'm first going to ask my questions of the Translation Bureau. I understand that this kind of remote assembly can be dangerous to interpreters because the sound quality is so bad. I'd just like to get a little bit clearer about what those dangers actually are for the interpreters.

Ms. Nathalie Laliberté: The sound quality, with the Internet connection and the sound varying from participant to participant, means that interpreters have to increase the volume, have to listen harder and have to concentrate harder. There's an increased risk of acoustic shock, or, as I said, when they come back from their assignment they have headaches, earaches and extreme fatigue. It makes it very difficult for them.

Their hearing is, really, how they work, so any damage to their hearing will mean that they will no longer be able to work. We have to be very careful with respect to protecting their health and safety. It's really a matter of the sound, playing with the volume and making sure they understand.

They're very dedicated. They will do their utmost to deliver the service, sometimes to the detriment of their own hearing.

Ms. Rachel Blaney: Have there been any increased injury or fatigue incident reports during the past month since Parliament committees have started, and now that the entire House is meeting virtually? If there have been, could you supply this committee with some numbers?

Ms. Nathalie Laliberté: There have been, yes, but we will have to come back to the committee with the exact number.

Ms. Rachel Blaney: Okay, thank you so much.

I would like to take this opportunity to speak with Microsoft for a quick second.

The witness from Zoom talked earlier about where information is stored. He said that all of the conferencing information from here would be stored in Canada. Where is your information stored when it comes to things that are happening in Canada, and specifically in the House of Commons?

Mr. John Weigelt: We commit to storing information in our data centres in Toronto and Quebec City, and those data centres are connected with fibre optic cable that runs within the country. We feel that is the differentiator for our services.

Ms. Rachel Blaney: Okay. I have another question.

Of course, what makes Canada specifically wonderful and unique is the fact that we have two official languages. It is an obligation of Parliament to always be representative of those languages. As a person who's only an English speaker, I think it's so important that, as we go through this, we protect and respect both of those languages.

One of the challenges is making sure that there are platforms with interpretation. Are there any plans to develop this particular part of your programming for a platform that would work for Parliament?

Mr. John Weigelt: We recognize that the Constitution upholds the ability to work in both official languages. We also recognize that the Translation Bureau is a unique Canadian institution that was formed to do translation in both official languages and has extended that to support 60-plus indigenous languages as well.

You can do that today using supplemental solutions. Having a variety of different channels over the same venue, as we heard, can be fraught with challenges. The voice clarity might not be what it needs to be. We're working hard to find a solution to build that into the platform.

One of the things to consider, as we look at the transformation that's under way, is the use of artificial intelligence-enabled transcription to assist the translators. Microsoft sees AI as a way to empower individuals, not replace them, so being able to do voice transcription can provide the prompt or support to translators. Imagine how language sounds when it comes through a drive-through terminal: You can hear a crackled voice and you can barely understand. We found that the AI tools can transcribe that exceptionally well and can provide that assistance to the great work that our translators from the Translation Bureau are doing.

Ms. Rachel Blaney: Thank you.

I'm going to Zoom next. I have two questions.

The first one, of course, is on interpretation. I understand that while we're using that right now, there is a bit of system.... I'm wondering if this is specific to Canada or if you're working to iron this out generally, because there are definitely some challenges with that service.

As my second question, I'm just curious how many people Zoom employs in Canada.

● (2010)

Mr. Harry Moseley: We introduced translation in October of last year as part of our platform, and we can have numerous different languages available on the platform. We also have real-time transcription and closed captioning for the hard-of-hearing and other services of that nature. I think that's the answer to your first part.

On the second part, I don't have the number of employees we employ in Canada, but I will make sure that we get that back to you tomorrow.

Ms. Rachel Blaney: That would be really helpful.

One of the particulars, though, is that translation services through Zoom are not perfect, so I'm just wondering about the improvements upon that as well.

Mr. Harry Moseley: With respect to improvements in translation, I actually had a call earlier today with your CIO and your CTO for the House of Commons and we're connecting them with our product team. I think that might have occurred already today, and we're looking to improve upon that.

The Chair: Thank you so much. That's all the time we have.

Next up is Mr. Duncan.

Mr. Eric Duncan: Madam Chair, in the second round do we have four or five minutes each?

The Chair: We didn't really agree on that.

Mr. Eric Duncan: I'm good with whatever. I'm going to set a timer for myself so that I actually leave a chance for the witnesses to respond.

The Chair: I think four minutes is good, if we want to end before 8:30. We'll set it for four minutes. Thank you.

Mr. Eric Duncan: I'm good with that. Thank you.

I want to address some of my questions to Zoom.

Mr. Moseley, do you have a contract with the House of Commons specifically or do they purchase what's available online?

Mr. Harry Moseley: We are working through the master services agreement for the House of Commons. This is not just purchased online; we have an account team resident in Canada that is working with members of the House of Commons.

Mr. Eric Duncan: Is there a copy of the contract that we would be able to see to review as a committee, or is that not possible yet or not signed yet?

Mr. Harry Moseley: I don't have the status on the contract. I suspect that it can be shared with you. I don't see any reason that it couldn't be, but that's not something I control.

Mr. Eric Duncan: I appreciate that.

Do you have any other contracts with the Government of Canada, or is it just with the House of Commons right now?

Mr. Harry Moseley: I would have to check. I don't remember off the top of my head.

Mr. Eric Duncan: I would appreciate that, whenever you get the chance.

You addressed some comments about the recent changes you made to the routing of data. I want to take another angle on data protection or what is done with data. We've heard different rumours, and maybe my question will give you a chance to address some of these.

Is it true that Zoom data is sent to Facebook, regardless of whether or not someone has a Facebook account? Can you discuss that?

Mr. Harry Moseley: We never send any data to Facebook. That is not true. There was device information collected through the Facebook SDK. When we understood that, we immediately changed it within 24 hours for the Facebook login.

Mr. Eric Duncan: Okay.

Mr. Harry Moseley: No meeting data, no subscription data, no content, no chat, no nothing went to Facebook.

Mr. Eric Duncan: I appreciate that.

The reason I'm asking these questions is that sometimes I get concerned about the precedents that we may set as we enter into these relationships. As we have other committees that are looking at privacy laws, I would just hate it if they came back and said that since the House of Commons does it and members of Parliament do it, it should be in law. It's those types of things.

Another aspect we hear about a lot is the sale of data or information to third parties for advertising. Do you do any of that whatsoever—any data, any marketing, anything?

Mr. Harry Moseley: Nothing. Zero, zilch, zip. We have no intention of it, never had, and never will. It is not our business model.

Mr. Eric Duncan: I appreciate that. Thank you.

I have a quick question for Citizen Lab.

We mentioned the Zoom platform, and the line that's been used about it is it's a “gold rush for cyber spies”.

Do you agree with that assessment? Is it a Zoom-specific problem, or are there many platforms that have similar gaps in the challenges that you and others have addressed in media reports and studies?

Mr. Ronald J. Deibert: The comment we made, the evaluation we made about Zoom, was earlier in April, on April 3. Then we released a second report on April 8. Subsequently we've had conversations with the company and the CEO. They've made some significant steps towards improvement and they've laid out a 90-day plan, so I think they should be commended for the steps they have taken.

As it stands now, we would still not recommend Zoom, especially for sensitive communications. For something like this, it's fine, and for something like Parliament itself, it's fine, but if you were having discussions in camera or in caucus, I would not recommend it at this time—

● (2015)

Mr. Eric Duncan: I apologize for cutting you off, but I have only about 30 seconds left and I promised Mr. Richards that I would give him that last minute or so, if I can, Madam Chair.

Sorry. I appreciate the context and the update on that.

Mr. Blake Richards: I'd like to move a motion and I'll explain it in a second.

I move that the committee invite the International Association of Conference Interpreters, Canadian division, and the Canadian Association of Professional Employees to appear at the first meeting of the committee in the week of May 4.

The reason for the motion is that we've received letters and a request to appear from both of those organizations, which represent some of the interpreters that are used in our proceedings. The information that is in those letters seems to differ somewhat from the things that we heard today. I think it would be incumbent upon us as a committee to hear from them just to get that perspective. I think there would be time to do so in the first meeting we have scheduled next week.

Madam Chair, it could be agreed by unanimous consent of the committee, or I would be happy to set the vote aside until the rest of the people with questions have a chance to do that. We can do the vote on this motion at the end of the meeting, if that is helpful.

The Chair: Mr. Richards, can you repeat the second witness that you would like to have called? I believe we did receive emails, but your sound was breaking up.

Mr. Blake Richards: Sure. The other organization was the Canadian Association of Professional Employees.

The Chair: Okay.

We have received these requests. I think they were just received yesterday, and some came today, so we are trying to figure out how to incorporate them into our study.

I don't know if we need to go to a vote. Are all members in agreement that we can try to incorporate them into our future panels?

Some hon. members: Agreed.

The Chair: Okay.

Mr. Richards, is that okay, as long as they are here before May 5?

Mr. Blake Richards: I'm certainly satisfied with that if there's agreement that we would hear from them. My suggestion would strongly be that that it looks like we have room that first time next week if that can be accommodated. Certainly, I would be good to have them maybe come for the first half of that meeting and then the second half of that meeting could be with the officials [*Technical difficulty—Editor*] and then come back to [*Technical difficulty—Editor*]. That would be my suggestion.

The Chair: Thank you for that, certainly.

Now we will start with Dr. Duncan, for four minutes, please.

Hon. Kirsty Duncan (Etobicoke North, Lib.): Good evening, everyone.

First of all, thank you, Madam Chair. Thank you all for being part of this. We appreciate your time and expertise.

I'm going to go to Mr. Weigelt first. Do you think remote voting is possible, and under what circumstances, please?

Mr. John Weigelt: Do you mean in the context of a virtual Parliament?

Hon. Kirsty Duncan: Yes, in a virtual Parliament.

Mr. John Weigelt: Microsoft is a very strong partner-driven organization. We have over 1,200 partners in Canada that help deliver solutions on top of our Teams platform. We do have partners that support virtual voting for communities, so we do believe that it's possible on our platform.

Hon. Kirsty Duncan: Thank you so much.

Mr. Moseley, do you believe that remote voting is possible? Do you think it's possible to adopt a secure remote voting system?

Mr. Harry Moseley: Yes, I do. As part of our Zoom platform, we have an ability to ask impromptu questions of the participants and get their responses in real time during the meeting.

Hon. Kirsty Duncan: Do both of you think there are ways to authenticate or safeguard a remote vote?

Mr. Harry Moseley: I'd have to think about that. I would like to come back with an answer. I believe we could authenticate the vote, but I'd have to confirm that.

● (2020)

Hon. Kirsty Duncan: Thank you.

Mr. Weigelt, do you think it's possible to authenticate a remote vote?

Mr. John Weigelt: Absolutely. Based upon our enterprise heritage, we leverage those credentials, that identification that you harness for your day-to-day work within Parliament. Being able to recognize that throughout the voting process, I think, is critically important.

Hon. Kirsty Duncan: Mr. Weigelt, what measures would you suggest to protect the integrity of the vote?

Mr. John Weigelt: There are a number of cryptographic measures that can be put in place to protect the integrity of the voting materials so they don't get tampered with along the way or after they've been cast.

Hon. Kirsty Duncan: Would it be possible to table with the committee what those measures would be?

Mr. John Weigelt: Absolutely.

Hon. Kirsty Duncan: Thank you.

Mr. Moseley, do you think an MP should have to authenticate their identity after casting a remote vote?

Mr. Harry Moseley: Well, they authenticated into the meeting. Therefore, we know who they are and as the vote is being cast by the MP, it's connected to the authenticated individual. So I don't think they'd need to further authenticate for the vote.

Hon. Kirsty Duncan: Can I ask professor de Clercy from Western a question. I don't see her.

Can you tell us which countries are using remote voting at this point?

The Chair: Sorry, that was a professor on the last panel.

No, actually, she is right there.

Hon. Kirsty Duncan: I hope that's not off my time, Madam Chair.

The Chair: No, it isn't.

Go ahead.

Prof. Cristine de Clercy: Madam Chair, thank you for the question.

I have not carefully tracked what other legislatures have moved to online voting. Some of the witnesses here have mentioned some like [*Inaudible—Editor*] for example.

Hon. Kirsty Duncan: Thank you, Professor de Clercy. I looked at the Inter-Parliamentary Union's website yesterday, which has been updated. It includes Belgium, Brazil, Chile, Poland, Spain and, I believe, it is also under consideration in the U.K. and Estonia.

Thank you.

The Chair: Thank you, Dr. Duncan.

Next we have Mr. Richards, for four minutes.

Mr. Blake Richards: Thank you, Madam Chair. I didn't realize I had another round. That's fine. I do have some questions, so I'm happy to take it.

With regard to the interpretation, I think our witness from Zoom was asked about translation and [*Technical difficulty—Editor*]

The Chair: Mr. Richards, if it's your phone, could you move that away again? There's a lot of static.

Mr. Blake Richards: Okay. I don't know. It wasn't that close.

The Chair: If that's what it is....

Mr. Blake Richards: Is it better now? Okay.

In regard to the platform that we are currently using, Ms. Blaney asked a question about translation. Translation and interpretation are in fact two different things, obviously, and the answer with regard to translation was that it is available, but simultaneous interpretation is another matter.

I've been told—and I have not verified this—that on Zoom and other available platforms simultaneous interpretation is not something that's available, and that the House of Commons has had to make some accommodations to piggyback on Zoom to be able to make simultaneous interpretation work.

I'll ask the Translation Bureau. Can you verify whether simultaneous interpretation is in fact something you're using through Zoom, or is it something where a workaround has had to be figured out?

Maybe I'll also give Mr. Moseley a chance to indicate whether simultaneous interpretation is something that's available on the platform.

Ms. Nathalie Laliberté: Thank you for the question.

The Translation Bureau is not responsible for the technological aspects related to interpretation. That question would be best directed to the House administration, to those responsible for multimedia.

Mr. Blake Richards: You're not aware of what the arrangements were, then?

Ms. Nathalie Laliberté: No.

Mr. Blake Richards: Okay. No problem. It certainly is a question that we can save, and we do have the opportunity again next week.

Mr. Moseley, [*Technical difficulty—Editor*] about translation. What about simultaneous interpretation? Is it available through the platform currently?

● (2025)

Mr. Harry Moseley: Madam Chair, thank you for the question. I'm not sure I understand what "simultaneous interpretation" is.

Mr. Blake Richards: Okay. I could probably best let our Translation Bureau explain it. I think I could explain it, but they would probably explain it better, so maybe I'll let them do that, but essentially the difference is that translation is—

Mr. Harry Moseley: I understand translation.

Mr. Blake Richards: Yes, someone speaks and translation is provided after they've finished speaking. In simultaneous interpretation, it's that as the person is speaking, the interpretation, the translation, is being done in real time, essentially.

Mr. Harry Moseley: Got it.

Mr. Blake Richards: If you want a better explanation, I can let the Translation Bureau—

Mr. Harry Moseley: No, I'm good now. Thank you.

Our simultaneous interpretation of the spoken language is real time, and it's done as part of the existing platform.

Mr. Blake Richards: It is. Okay.

Mr. Harry Moseley: There are no add-ins to that.

Mr. Blake Richards: As you're speaking, I can be hearing what you're saying in another language at the same time.

Mr. Harry Moseley: That is absolutely correct. We've moderated it at 20% of the speaker and 80% of the translator. The reason we do that is so you can hear the tone of the speaker as well as the words.

Mr. Blake Richards: Okay. Thank you for that clarification.

Let me just see here. What else did I have? I put my notes away, but I do have some other questions I wanted to ask. I guess probably back with the Translation Bureau again—

The Chair: That's about all the time we have.

Mr. Blake Richards: Okay.

The Chair: I think I could further clarify that translation is, I believe, in writing. Interpretation is oral. Is that, right, Madame Laliberté? Okay. That's the difference between translation and interpretation: one is oral and one is written.

We'll move on, though, to Madame Petitpas-Taylor. There has been a request by Ms. Blaney to complete this whole second round, so after that we'll have two minutes for Madame Normandin and two minutes for Ms. Blaney.

[*Translation*]

Hon. Ginette Petitpas Taylor: Thank you, Madam Chair.

I have a comment and, then, a question. I'll be switching languages.

Ms. Laliberté and Mr. Ball, I'm certain that I speak for my fellow members when I say thank you. We appreciate the services you provide to the House of Commons every single day.

I'm from New Brunswick, Canada's only bilingual province, so please know that both official languages mean a lot to me. From the bottom of my heart, thank you for the work you do.

[*English*]

Mr. Moseley, yesterday I realized there is a new verb out there called "zooming"; we've been doing an awful lot of zooming lately.

I'm wondering if you would be able to tell us what steps Zoom is taking to protect our personal data. We've heard a lot of about that in our first session today.

Also, could you talk to us about what steps you are taking to protect our privacy?

Mr. Harry Moseley: Security, privacy and protecting data is paramount at Zoom. As I mentioned in my opening remarks, we take that very seriously. It is one of the four core principles Zoom is built on.

We've made an abundance of changes as part of the 90-day plan, which has been referenced a couple of times in this session, most notably the upgrade to our AES-256 GCM encryption, which is the highest level of encryption service. Everything is encrypted from the digital device from the time it leaves the platform all the way through the network, through our data centre until it reaches the destination. Everything is fully encrypted at rest. We have defaulted to complex passwords. We have defaulted waiting rooms. Moreover, if you did a cloud recording, we have defaulted to having that with a forced complex password as well.

● (2030)

Hon. Ginette Petitpas Taylor: Did I understand we can purchase additional security features to make sure that added security measures are in place?

Mr. Harry Moseley: The encryption services, the security services, are paramount and they are part of the existing platform in its entirety. We take it very seriously.

Hon. Ginette Petitpas Taylor: That's great.

John, I'm curious to know how many employees Microsoft has in Canada?

Mr. John Weigelt: We have over 3,200 employees in Canada with very strong development capabilities in Vancouver. And Microsoft Research in Montreal is doing leading edge research in AI and AI use in languages. We're quite proud of that.

Hon. Ginette Petitpas Taylor: That's great.

Thank you.

That's all, Madam Chair.

The Chair: Thank you.

The clock says 8:31.

Ms. Normandin, Ms. Blaney, I really want to give you the time but they're telling me they need to clear the room.

Is it okay if we call this meeting to a close today?

Perhaps we can work something out for tomorrow's meeting. I know there won't be the same witnesses, of course, but...

That is the end of the meeting. There are a couple of housekeeping things to do. I'm going to flag them today because we don't have enough time and we can discuss them tomorrow if needed.

The next meeting is on April 30 and the first panel will be other parliaments or institutions. The second panel will be procedural, legal and constitutional witnesses.

I also want to remind everybody to start thinking about recommendations for the final report. We will only have about two meetings to discuss the draft report. As much as possible, could we start thinking about that or if there are going to be any dissenting reports?

But we can speak about that tomorrow.

Yes, Ms. Blaney.

Ms. Rachel Blaney: I was just going to ask if there's a timeline for having those recommendations in? I think that would be helpful.

The Chair: I've been informed by the analyst that by May 7 or so, he may be able to have a little bit of a draft report done, but then by May 11 we should have the complete draft report done. We will have two days after that, and we need to have everything completed ideally by May 13 to get our report done for May 15. That includes dissenting reports and all of our recommendations, and allowing enough time for translation so that we can submit on May 15. We can discuss that a little bit more tomorrow if you like and we can carve out some time for that.

In conclusion, I want to thank all of the witnesses. This was a very enlightening panel. We've learned a lot.

You will see that your submissions and what you've said here today will be a large part of our report and recommendations to Parliament.

Thank you and good night.