



HOUSE OF COMMONS  
CHAMBRE DES COMMUNES  
CANADA

43rd PARLIAMENT, 1st SESSION

---

# Standing Committee on Procedure and House Affairs

EVIDENCE

**NUMBER 022**

Thursday, June 11, 2020

---

Chair: Ms. Ruby Sahota





## Standing Committee on Procedure and House Affairs

Thursday, June 11, 2020

• (1105)

[English]

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

Welcome to meeting number 22 of the House of Commons Standing Committee on Procedure and House Affairs.

The committee is meeting on its study of parliamentary duties and the COVID-19 pandemic. Pursuant to the motion adopted by the House on May 26, the committee may continue to sit virtually until Monday, September 21, to consider matters related to COVID-19 and other matters.

Certain limitations on the virtual committee meetings held until now are now removed. As mentioned, the committee is now able to consider other matters, and in addition to receiving evidence, the committee may also consider motions as we normally do. As stipulated in the latest order of reference from the House, all motions shall be decided by a recorded vote.

Finally, the House has also authorized our committee to conduct some of our proceedings in camera, specifically for the purpose of considering draft reports or the selection of witnesses. On this point, however, I would like to clarify that the Clerk of the House has informed the whips that, until the House administration finalizes a process to switch between public and in camera proceedings within the same meeting, all virtual meetings that begin in public must remain in public until the end, and all virtual meetings that begin in camera must remain in camera until the end.

Today's meeting is taking place by video conference and all the proceedings will be made available via the House of Commons website. The webcast will only show the person speaking, rather than the entire committee.

To ensure an orderly meeting, I would like to outline a few rules to follow. Interpretation in this video will work very much like in a regular committee meeting. You have the choice, at the bottom of your screen, between either floor, English or French. As you are speaking, if you plan to alternate from one language to the other, you will also need to switch the interpretation channel so it aligns with the language you are speaking. You may want to allow for a short pause when switching between languages.

Before speaking, please wait until I recognize you by name. When you are ready to speak, you can click on the microphone icon to activate your mike.

This is a reminder that all comments by members and witnesses should be addressed through the chair.

Should members need to request the floor outside 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 me your interest to speak. To do so, you should click on the "participants" icon on the toolbar below. When the list pops up, you will see the "raise hand" function next to your name, but for some it may be at the bottom of the participant toolbar.

Please speak slowly and clearly. When you are not speaking, please ensure your mike is on mute.

Headsets for all our witnesses are strongly encouraged. Of course, all members of Parliament already know this.

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 the problem. Please note that we may need to suspend during these times as we need to ensure all members are able to participate fully. We have had some of these issues occur in the past. Please try your best to inform me or the clerk that you're having some difficulty so we can try to get you back online or get your audio working.

During this meeting, we will follow the same rules that usually apply to opening statements and the questioning of witnesses during our regular meetings. The witnesses will have seven minutes for opening statements and that will be followed by two rounds of questions by the members. As usual we will suspend between panels to allow the first group of witnesses to depart and the next panel to join the meeting.

Before we get started, can everyone please click on the top-right side of their screen and ensure they are on "gallery view"? With this view you should be able to see all the participants.

Without further ado, I would like to welcome the witnesses. This is a long-awaited panel. There have been a lot of questions surrounding security and IT.

We're very happy to have our witnesses today: Mr. Essex, associate professor at the University of Western Ontario; Madam Goodman, assistant professor at Brock University; Mr. Roberge, president of Arc4dia; and Mr. Morden, research director at Samara Centre for Democracy.

Thank you so much for being with us today.

Can we begin with Mr. Essex, please?

**Mr. Aleksander Essex (Associate Professor, University of Western Ontario, As an Individual):** Good morning and thank you, Chair.

Thank you for this opportunity to speak to the committee.

As I was preparing for this statement, my son reminded me that a group of owls is called a parliament, so let me say what a hoot it is to be here this morning.

My name is Aleksander Essex. I'm an associate professor of software engineering at Western University. My research is in cybersecurity and cryptography, but my expertise is in the cybersecurity of elections.

I've studied cybersecurity issues of online voting extensively in Canada and abroad. I frequently share these findings with election agencies and commissions, municipal councils and associations. I co-authored the 2013 cybersecurity analysis of vendor proposals for the City of Toronto regarding their online voting RFP. I led a cybersecurity study of online voting use in the 2018 Ontario municipal election. In February I spoke at the New South Wales parliamentary committee on electoral matters about their online voting system. Next month I'll be speaking to a Northwest Territories legislative committee about their new online voting system.

More recently, I've been working with Dr. Goodman—who's speaking next—to try to advance the cause of cybersecurity standards for online voting in Canada. Our country actually has one of the highest rates of online voting use in the world, but somehow we have no standards for any of it. As you can imagine, this has led to a number of troubling incidents and, in my opinion, a very intolerably high cyber-risk exposure.

I've seen a lot of bad voting technology in my time, so back in March, when Dr. Goodman and I heard that Parliament was studying the issue of remote legislative voting, we wanted to get out in front of any potentially dubious proposals, such as the EU Parliament's idea to use email for voting. We wrote an article in Policy Options to try to provide some food for thought. It was interesting, because although the article was about how to do remote legislative voting in a safe, cyber-conscious way, all the feedback we received revolved around the importance of parliamentary tradition.

I agree that parliamentary tradition is really important, but our present circumstance isn't exactly traditional. The Globe reported this week that there have been 38 regular sittings of the House in the past 12 months. That's not tradition. There were 30 members voting on historic spending measures. That's not tradition. All the members were meeting in a kind of supercommittee but not actually voting. That's not tradition either.

Here we are. What are we going to do?

The good news is that remote legislative voting happens to be a way easier technical problem than online voting for general elections. There are a couple of good reasons for that. One is that unlike a general election, Parliament can support MPs with secure technology and training. Most importantly, legislative votes are not secret. They're a matter of public record. That means you can go back and

check what was recorded. It means you can actually detect when things go wrong.

Here's where we have to be careful: It's not enough to be able to check. You need to actually do it, and you need to have procedures in place so that you know what to do when things go wrong.

This might seem like a totally obvious statement, but it's actually not. I mean, it should be, but our experience has demonstrated, time and again, a kind of bias in the election world to, frankly, only prepare for disasters after they've already happened. We're saying let's not wait. Let's anticipate. Let's build it right from the beginning.

Let me give you an example. Six months before the 2018 Ontario municipal election, I did a story with CBC about how I was worried that the cities that were doing online voting didn't seem to have a cyber-incident response plan. Imagine the Internet goes down on election night; what are you going to do? What's your game plan? CBC then went and interviewed a number of city clerks. Several of them admitted that they actually didn't have a plan. One even literally said that they were hoping nothing happened.

What do you think happened? One of the online voting vendors accidentally didn't provide enough bandwidth. The online voting websites of 43 different cities, accounting for almost a million voters, went down on election night, and 35 of those cities used emergency measures to extend the voting period by 24 hours. It wasn't just that these cities didn't have a plan in place. It's that they didn't think it was enough of a risk to even have a plan for it.

● (1110)

You might think that this was just a fluke, but a similar situation happened in New South Wales last year, which is why I was testifying there. I was telling them about what happened in Ontario because it was related. Their registration went down on the eve of the election. You might think that this is all good, that this all applies to general elections, that legislative voting is different. However, just last week in Sarnia, Ontario, a city council vote actually passed by mistake. It turns out that the word “disagree” sounds exactly like the word “agree” if the first syllable drops out in a glitchy Zoom connection.

Fortunately, the staff was on the ball, and they caught it this time, but what about next time? Obviously, we need procedures to make this kind of checking repeatable and, by the way, part of the ultimate eventual tradition.

We have only touched on accidents and mistakes, but we're also worried about deliberate efforts from advanced persistent threat actors like nation states. We have seen these kinds of advanced threat actors living in the IT infrastructure of our cities. If they're willing to spend months mapping out a system for a few thousand dollars of potential ransom money, imagine what they could do to an election. Then, why even hack an election when you could just hack the law itself?

Let me conclude by summarizing a few takeaways. Secure, remote online voting for non-secret parliamentary divisions is doable, but it has to be done right. There have to be procedures for detecting errors, whether they are due to hacking or accidents or disasters. Someone has to be responsible for checking that an MP's vote was correctly recorded. There have to be procedures for granting opportunity to recover from that error, and we have to confront our temptation to think that nothing is going to happen.

I heard that people were talking about tornadoes last night and windows blowing open, and these sorts of things don't happen until one day they do.

Madam Chair, thank you for letting me share these thoughts with you. It would be an honour to answer any questions the committee may have.

Thank you.

• (1115)

**The Chair:** Thank you. We appreciate that.

Go ahead, Dr. Goodman.

**Ms. Nicole Goodman (Assistant Professor, Brock University, As an Individual):** Good morning. I'd like to begin by thanking the chair and members of the committee for the invitation and the opportunity to speak today and share my research and thoughts.

I've spent the past 11 years working in the area of electronic voting, both within Canada and internationally. This work has involved leading and co-leading projects to examine the effects of remote online voting in the context of municipal elections, indigenous elections and a range of political party votes. Beyond social and political effects, I have been looking at the cybersecurity of digital voting from a policy perspective and exploring regulatory possibilities. Much of this work has involved collaboration with my colleague Dr. Essex.

Today I'd like to make four specific points: one, why online voting works for legislative voting; two, the types of remote electronic voting that could work in a legislative context and which one is best for Canada's House of Commons at this time; three, how this work could make the legislature more flexible and accessible in the future; and four, some opportunities for thought leadership.

To begin, I'd like to provide the committee with some context about the core debate surrounding voting remotely over the Internet.

There are two primary sides of the debate, which usually focus on deployment in public elections. On the one hand, there are arguments for the benefits of online voting, such as enhanced accessibility, convenience and increased turnout. These benefits have been

documented in municipalities and first nations in Canada. On the other hand, however, there are concerns about the cybersecurity and privacy of the vote. In some instances, online voting trials supporting public elections have been halted or cancelled due to security concerns or the detection of vulnerabilities. Two examples include a system in Switzerland and one in New South Wales, Australia.

This debate is relevant for the committee's consideration because remote online voting can support Parliament to continue during the pandemic without sacrificing representation and the inclusion of members. At the same time, there are unique characteristics about legislative voting that make remote online voting possible and the cybersecurity more solvable than in public elections. As my colleague mentioned, the reasons for this are outlined in our brief to PROC: An MP's vote is a matter of public record, and the federal government has the resources and capacity to support the cybersecurity infrastructure and implement necessary policy and procedures.

Based on our review, there are four main types of electronic voting that could enable remote voting for MPs. There's email voting, where members receive a ballot form electronically via email and submit their votes via email. This approach is being used in the EU Parliament. There's web-based voting, which is used in public elections and party votes in Canada. This involves ballots being accessed and cast via a website. An example of this is the U.K. House of Commons' MemberHub system. There's application-based voting, where members download an application to access and cast ballots. The Chamber of Deputies in Brazil has taken this approach. There's also video voting, where members vote via video by a show of hands or by voice. This is being used by local councils across Canada. Belgium, for example, is also using this for its committee votes.

All of these approaches have benefits and challenges, with email voting being the least secure and posing the greatest risk. In a legislative context, video voting presents probably the best or most usable solution for regular non-anonymous parliamentary votes. There are some benefits to this approach: It poses less risk, although there are still risks that need to be managed; it is the easiest to deploy and requires less technology; and it interfaces more closely with the parliamentary tradition of standing in the House.

Implementing video-based voting would require establishing some procedures. Here are some examples.

One is establishing whose responsibility it is to watch and record a vote. This could include staff members, MPs, party whip offices or perhaps a special segment of staff who support digital House matters. One consideration here is to think about putting a process in place where votes are double verified either by two individuals or across two different areas.

Another example would be mandating neutral backgrounds in video conferences to ensure that there are no images in the background that could send messages or carry a partisan tone that couldn't be visually signalled in the legislature.

A third example would be allowing the Speaker to call for a revote in the case of technical errors. This was a procedural change introduced in the U.K., for example.

This does not mean video voting is without challenges or would work in all contexts. Anonymous votes, for example, would not replicate well on Zoom.

My third point has to do with making the legislature more flexible and accessible. Enabling a system for remote online voting could have future benefits in keeping legislative business moving in times of crisis, such as with COVID-19, climate change and future viruses, and in the context of accessibility for individual MPs.

- (1120)

The option of remote online voting could provide MPs with improved access to voting under special circumstances, such as in situations of maternity leave or parental leave following the birth of a child; in times when an MP's constituency is faced with a specific crisis, and they are torn between being in their community or advocating for their constituents' interests in Ottawa; or in cases of sickness where a member is not able to physically attend the legislature.

This committee considered proxy voting and electronic voting in 2016 as part of a study on how to make the legislature more family-friendly. However, no recommendations were made at that time. Other legislatures, like the U.K. House of Commons and Australia's House of Representatives allow for proxy voting for new parents, while Canada's House of Commons currently requires a member to be present in the chamber to have their vote recorded.

I understand that witnesses have been unanimous that the committee consider these changes for the pandemic only. However, thinking about how such a system could enhance the participation, representation and inclusion of members in certain circumstances is part of modernizing the legislature.

In closing, while the committee does not have to engage in a typical online voting debate, we see with regard to public elections, it does have to engage in its own debate about maintaining parliamentary tradition versus modernizing to become agile in uncertain times.

Finally, there are two opportunities for thought leadership. The committee's work in this area on policies and procedures for remote voting could not only benefit the House of Commons in the future but also other legislatures across Canada and abroad.

There is currently no regulation of remote online voting in Canada, so as we think about the adoption of voting technologies in the legislature, we might also reflect on how this conversation could later benefit electoral integrity in the context of public elections.

Thank you.

**The Chair:** Thank you so much, Dr. Goodman.

Next we have Mr. Roberge.

**Mr. Pierre Roberge (President, Arc4dia):** Thank you very much, Madam Chair and members of the committee, for inviting me to participate.

I will start with a bit about me. I have worked in cybersecurity, facing the most advanced cyber-attacks in the world for the past 20 years, both within government and as an entrepreneur. I am currently leading Arc4dia, where we are providing services, acting as the last line of defence to detect intrusions by leveraging our proprietary software. We have been operating remotely and decentralized since I founded Arc4dia 10 years ago. I also participate within the Bitcoin community, both publicly and within invitation-only fora, as a think tank in security and game theory in the ecosystem.

I came with a few points to share with this committee from listening to the previous meetings. Although I only listened to a few, I do have some observations.

I observed a resistance to change that is driven by a desire to keep what works well, and that, due to past errors, hurts collegiality. It is true that change is a threat vector that can be exploited by others. However, being static is also a weakness that can be exploited to prevent us from fixing what we have broken in the past or what needs to change in order for us to adapt. With the world changing around us, and very fast, with the rise of artificial intelligence combined with cyber-domain attacks and social engineering driven by artificial intelligence, I believe we need to change and adapt and, even better, be ahead of the curve.

To do so, and to dwarf non-genuine influences, we need to strengthen collegiality. It is by knowing each other more intimately that we will detect and see attacks against us and have the agility and the speed necessary to react before damage is done. For example, limiting or reducing face-to-face interaction has been brought up by many during the hearings as a change that will have negative outcomes for the effectiveness of our democracy. These are the kinds of changes where we need to be agile and be able to bring back collegiality. I heard that some get-together dinners were removed from the tradition of the House of Commons, where opposing parties had held discussions in a more relaxed and convivial atmosphere. I would advise you that such sittings are very important in our defence against cyber-domain attacks.

Understanding the nuances of our interpersonal and professional communications is essential in detecting subtle attacks against us. Our adversaries will look for ways to interfere with all forms of communication, and not just the written kind in email, texts and online postings. For example, during video-based presentations they will or could disrupt images and the tone of voice in an effort to inject or alter messages of body language, facial expressions and the intentions of our elected officials. Without our collective understanding of what right looks like, we will fail to see the subtle attacks that will eventually lead to more brazen and flagrant attacks.

I also observed concern with e-voting. E-voting and the use of technology should complement and reinforce one vote. Make sure your voice can be heard and make sure it is accurate. The way I see technology and software is that they augment our reliability and agility in our voting process, and perhaps even make it antifragile. We need to move away from using a single platform to vote, in favour of adding technological compatibilities to strengthen the reliability and the resiliency of voting. Perhaps we should vote on video, as well as signing our votes with dedicated, secure hardware. We can then audit that our votes are correct. Perhaps we could time-stamp our votes with a Bitcoin blockchain, making them forever verifiable.

In short, diversity—one might say multifactor authentication—in our methods of conducting business face to face, by voice and electronically will make it more difficult for our adversaries to achieve their desired outcomes and improves our opportunities to detect their attacks. These ideas and improvements should come gradually, holistically and in an agile process. If not already in place, I would recommend that the House of Commons put in place such processes, supported with permanently ongoing threat and risk assessment, versus the typical static evaluation that ends up on the shelves collecting dust to check some accreditation marks.

In closing, the three observations I have described are woven together by a common thread; that is to say, defending ourselves is more than simply a technology issue. To protect the integrity of the House of Commons and the parliamentary process so that legislation, policies and directives of the Government of Canada truly represent the intentions of the electorate, we need to provide the electorate with the highest level of confidence that the actions of the House of Commons are truly what they are supposed to be.

- (1125)

Regardless of the method of operation, whether it is in person or virtual, the importance of this cannot be overstated.

We require defensive measures, assessed and developed in a holistic and continuous threat-risk managed manner that address all forms of attacks, such as political attacks on infrastructure and people, attacks that attempt to compromise the integrity and loyalty of our people, attacks that attempt to compromise or disrupt the integrity of our supply chains, attacks aimed at disrupting our ability to determine truth from fiction, and of course, attacks that attempt to disrupt or compromise our IT systems. There is no higher calling than to protect our democratic institutions and our country.

I thank you, and I look forward to your questions.

**The Chair:** Thank you, Mr. Roberge.

Mr. Morden.

**Mr. Michael Morden (Research Director, Samara Centre for Democracy):** Thank you, Madam Chair, and thanks so much to the members of the committee for this opportunity to address you.

My name is Michael Morden. I'm the research director of the Samara Centre for Democracy. The Samara Centre is an independent, non-partisan charity that is dedicated to strengthening Canadian democracy through research and programming.

We want to thank the committee for undertaking this study. Given the scope of the crisis, the scale of the government's response and the enormous uncertainty that exists, Parliament is not optional at this time. The only question to address ourselves to is how to make it work. Arriving at a solution that commands some measure of cross-partisan support is a solemn responsibility that falls to you.

I understand that our presentation comes perhaps somewhat late in your deliberation. Nevertheless, I think it's useful to consider questions of politics and principle at the same time as technical ones, to remember why we're pursuing this, and not to miss the forest for the trees.

The Samara Centre supports a move in the immediate term to hybrid virtual and in-person sittings of the House of Commons, with remote voting for those who are unable to attend in person. We think the hybrid virtual model is the best among imperfect options.

To be clear, the best of all versions of the House of Commons is the one in which 338 individuals share a room, and there are a lot of reasons for that. We've been a consistent voice in calling for members to spend more time together in Ottawa, to facilitate collegiality and to build informal relationships between members, parties and chambers. However, given the limits imposed through physical distancing, and credible concerns about travel, in our assessment, that option just isn't on the table. We need a full-service Parliament now and, in our view, through the summer.

I hope the option of a full, in-person convening of the Commons will return soon, but we're clearly in a state of deep uncertainty. As the second-largest country on earth, we may find that we're uniquely challenged to get back to full physical national sittings of Parliament. It's a necessary step in the immediate term and a prudent step for the middle term to institute the capacity to resume full parliamentary business with remote participation.

I want to foreground the values that lead us to that conclusion. In times of uncertainty, it's often worthwhile to return to first principles. Parliament exists for scrutiny, to enable the passage of legislation and also for democratic representation. The most desirable pandemic Parliament is one that strikes an appropriate balance between all of those functions. We feel that the current approach, employing a handful of day-long sittings in addition to committee work, is not sufficient to deliver the level of scrutiny, productivity and representation that's required.

We also take issue with any approach that would convene the Commons but exclude most of its members, for example, by operating on the basis of a skeleton crew of 40 or 50 MPs. That approach facilitates some scrutiny and enables the passage of legislation, but in our view, it comes at the expense of democratic representation. Some 18 million Canadians voted last fall to send individual representatives from each of their communities to Ottawa, and it's no small thing to render the vast majority of those communities unrepresented in the Commons while these momentous decisions are being taken.

For that reason, we think the best balance between scrutiny, productivity and representation is struck with a hybrid Parliament permitting remote participation, including remote voting. The technical challenges posed by such an approach are not insurmountable. Many other jurisdictions have walked this road. There are different models available to us, as Dr. Goodman described, and the House of Commons administration deserves particular praise, in our view, for adapting and adding capacity with alacrity.

In our view, there's no question that remote voting is feasible. It's feasible to do it securely, and it only awaits a decision by parliamentarians.

In the early stages of the pandemic, we supported the notion of incremental adaptation. Moving to a hybrid virtual Parliament was never going to be as simple as flipping a switch. We now have proof of concept, both in the experience of other jurisdictions and also in Parliament's own experience of authorizing the virtual conduct of some business activity. At this point, we hope that the committee will provide the Commons with a strong prompt to move as quickly as is feasible to resume full parliamentary business with remote participation.

• (1130)

We believe that legislative business should not be limited to the pandemic response alone. We welcome the granting of committees the opportunity to discuss other issues. We would like to see that reflected in legislative work as well. There are a range of issues that were urgent in January and February of this year that are no less urgent now. Just as doctors warn about the possibility of secondary health crises that are a consequence of delaying treatment for non-COVID-19-related illness, Canada may also become vulnerable to multiple crises during and after the pandemic if we can't attend to the policy needs that existed before it.

We also believe that the hybrid virtual Parliament's business should include opposition days and private members' business. No one has all the answers right now, so this is a really good time for multiple inputs.

In closing, I want to mention briefly that the Samara Centre periodically surveys MPs, and we're doing so now precisely on the question of how the pandemic has affected and should affect parliamentary work. We're always keen to develop an accurate picture of members' views on this issue and develop a body of evidence, and we encourage all members to make use of this anonymous platform to share your expertise.

Thank you very much.

• (1135)

**The Chair:** Thank you, Mr. Morden.

We will continue into the questioning portion of this panel. We will start with Mr. Richards for six minutes, please.

**Mr. Blake Richards (Banff—Airdrie, CPC):** Thank you.

I will start with Dr. Essex and Dr. Goodman.

I listened to some of the comments made by Mr. Morden just now. In your opening remarks, both of you talked about voting. You expressed your concern about voting for electoral events being

done electronically, but indicated maybe it could work in the parliamentary context.

I guess I didn't hear from either of you any thought about some of the other things that lead into voting. You talked about the technicalities of it, and that's important too, but a lot of things lead into it.

Mr. Morden was talking about some of those other things that occur in Parliament besides, obviously, just the voting aspect of it. Things like debates go on in the House, and we have the input we get from constituents, consultations we have and discussions we have within our parties and within our caucuses. Committee studies happen, all of these things, and then there's even the stuff that happens in the hallways, the corridors and whatnot. Mr. Morden identified how important some of those things are.

I want to see if either one of you has given any thought to those things and, when we're dealing with online or remote voting, whether there would be an impact on those things and what that might mean for democracy or for Parliament.

Dr. Goodman or Dr. Essex, do either one of you have comments?

**Ms. Nicole Goodman:** Obviously, the ability to engage in parliamentary debate is central. It speaks to the scrutiny function that Mr. Morden spoke to about presenting motions.

My testimony focused more on the voting aspects, like you said, but that's not to negate the importance of those functions. I don't think they can be replicated in an online setting the way that they take place in the legislature, and I certainly wasn't advocating for that, but I think we need to be able to find a workaround in the interim to keep representation moving and ensure that we're not having these modified sittings with a few MPs where representation is compromised.

**Mr. Blake Richards:** Sorry, I don't mean to interrupt, but I will, because you raised something I wanted to follow up on. You said we need to have a workaround in these kinds of situations.

Would you be advocating this as just a solution for these types of emergency situations, or do you believe that this would be something that would become permanent or should become permanent?

**Ms. Nicole Goodman:** I definitely think this is a solution for emergency situations, definitely times of crisis. My point was that we have a crisis now, unfortunately, which presents challenges but also presents opportunities. That's not to say we won't have a crisis in the future.

Government too often is reactive instead of proactive, so let's use this time to develop a thorough, robust solution for emergency situations, because there could be another virus, there could be a revisitation of the COVID rates increasing and there could be an issue of climate change.

My only point about considering modernizing the legislature was specifically enabling remote voting or considering enabling remote voting for specific circumstances that individual MPs may be in, but I definitely am part of the camp that believes that Parliament functions best when members are in the House actively debating and engaging.

**Mr. Blake Richards:** Okay. Thank you.



Maybe just really quickly, Mr. Morden, given those concerns that you raised about some of the other functions of Parliament and how difficult they might be to function appropriately, do you have concerns about the thought of things like virtual sittings or remote voting becoming permanent?

**Mr. Michael Morden:** What I have received from these deliberations is near-universal consensus that these should be temporary measures. I think it's important that members bear in mind the potential negative consequences. We don't want to diminish the costs, which we think are real, but this isn't, in my view, about modernization. It's really more a radical adaptation for a radical time, which we hope won't persist.

I think we can feel relatively comfortable. I reject the notion of a slippery slope in that I'm fairly confident, based on the deliberation I have heard from members, that they are able to distinguish these times from normal times and would prefer to return to a normal Parliament as soon as possible. I think we have to do what we've done in so many sectors, which is to embrace choices that wouldn't be acceptable in a normal time.

• (1140)

**Mr. Blake Richards:** Okay. Thank you.

Maybe I'll turn to Mr. Roberge.

I wonder if you, as an expert in security, could just give us some thoughts on the threats that would be there for both virtual sittings of the House and remote voting. What would be the differences in the sources and types of those threats between those two things, between the idea of televised debates and then off-camera electronic voting?

**Mr. Pierre Roberge:** Right. Without going into that we cannot really replace the beer time and get-together time, the social angle of the debate, technically I think it will be possible.

I don't know that it is at the moment, but at the speed that artificial intelligence is going, if we're not careful, it would be possible, eventually, to do deepfakes during video conferencing, potentially.

**The Chair:** Thank you, Mr. Roberge. That's all the time we have.

Next up is Mr. Turnbull.

**Mr. Ryan Turnbull (Whitby, Lib.):** Thank you to all of the witnesses for being here today. I really learned a lot from your testimonies.

I'm going to start with some questions for Mr. Essex and Ms. Goodman.

I read your article in Policy Options. I thought it was a really big contribution to this dialogue. Both of you, I assume, based on your testimonies today, still agree with a quote in the article that "Parliamentary voting...is entirely workable from a cybersecurity perspective".

Would you say that you still stand by that claim, Mr. Essex?

**Mr. Aleksander Essex:** There was a bit of editing that went on after the fact, but what I am simply here to say is that, compared to the cybersecurity risks of online voting for general elections, online voting for legislative or parliamentary divisions doesn't pose the

same sort of basket of threats. It is possible to do with careful design.

**Mr. Ryan Turnbull:** I got that, and I'm going to ask you more questions about that in a minute because I think it's essential to make that distinction.

Ms. Goodman, would you say that you stand by that quote or that claim?

**Ms. Nicole Goodman:** Yes. I would echo what my colleague, Mr. Essex, articulated, which is that there are obviously challenges that cybersecurity experts and the cybersecurity community raise with respect to secret ballots in public elections. Because it is an open public vote, we're able to overcome some of those in a legislative context.

**Mr. Ryan Turnbull:** I got that, yes. Legislative voting or parliamentary voting is highly distinct from general elections.

I know your work. Both of you have done a lot of work on electronic voting for general elections, but you make the distinction in that article, which I thought was really important for this debate and discussion, that parliamentary voting is a matter of public record. By virtue of that, it's transparent and open. It poses less risk for interference. I think there is a really important claim to be made there.

You also mentioned two other points that I thought were important. You didn't stress those as much, maybe, in your opening remarks, so I'm going to ask you some more questions about those. You also said that the federal government has the cybersecurity infrastructure to do remote online voting for legislative purposes.

Can you tell me a little more about what you know about the cybersecurity infrastructure? We've heard from other witnesses that it's highly robust. I am satisfied as a member of Parliament that it's really robust, but I wonder if you could fill us in on anything you know.

**Mr. Aleksander Essex:** When we said that, we were speaking as members of the public looking inside at what is ultimately a mostly opaque infrastructure—the intelligence community, the CSE. We don't really know exactly what they do, but we do know that they're there and we do know that they have a mandate to provide security services for government.

I don't think, if you were a municipal council, you would have access to that level of assistance—

• (1145)

**Mr. Ryan Turnbull:** But it's certain that it's world-class cybersecurity infrastructure; are you fairly confident that this is what exists on Parliament Hill and that the House of Commons is generally very secure in terms of its IT infrastructure?

**Mr. Aleksander Essex:** I never say something is secure until I have an opportunity to examine it. I don't really know what Parliament does, but my expectation is that as a Five Eyes member, we would have top world-class cybersecurity. I've spoken to the CSE before. They are very capable, but again, as a member of the public...you know.

**Mr. Ryan Turnbull:** Thank you.

I want to ask about the other point you made, about the distinction between these two types of online voting. The federal government generally has the capacity to train MPs on the new procedures. It's clear that the federal government has a lot more capacity than maybe other levels of government.

Ms. Goodman, do you want to speak a little about why that's so important and why that's important for this distinction?

**Ms. Nicole Goodman:** Absolutely. I believe when we wrote the article, we were framing it in the context of perhaps web-based or application voting, where you would go on a website and click. Maybe the intent is signalled a little bit more easily there, but upon reflection, I do think that video voting would work better for Parliament, for the reasons outlined.

**Mr. Ryan Turnbull:** Good; I was going to ask you that. You mentioned four different types of electronic voting, but I noticed you focused on the video voting. You made a claim about email voting being the least secure, but you didn't cover web-based or application-based, and I wondered why you shied away from that.

You know, I think video voting, which we've had some conversation about, is probably the easiest to implement. As you said, it might most closely mirror how we vote in the chamber. At the same time, is there not an opportunity here to develop an application or have a web-based voting system like the one that the U.K. developed, which, as we've heard from those witnesses, was quite robust?

**Ms. Nicole Goodman:** That is an excellent, excellent question. Just really briefly, with respect to procedures, for any remote online voting system that Parliament were to adopt, we would require procedures.

With respect to the article, we were really talking about cognitive biases and ensuring that the proper procedures were in place so that MPs could check their vote and ensure that that was how they intended to vote. As you heard from Alex, even in the case of Sarnia, where there's video voting, there was a glitch that flipped the vote the other way.

**The Chair:** Thank you, Dr. Goodman. That's all the time we have.

Next up is Madame Normandin.

[*Translation*]

**Ms. Christine Normandin (Saint-Jean, BQ):** I thank all the witnesses very much. Hearing from them has been especially useful and meaningful. I will try to ask a number of questions. The first is for Mr. Morden.

Mr. Morden, you said that Parliament was not optional and that we will end up with delays in terms of decision-making. I would like to hear your thoughts on the fact that Parliament is technically supposed to reopen on September 20.

How important is it to already have a voting system in place by September 20?

[*English*]

**Mr. Michael Morden:** I'd like to see a voting system in place even before then. I think there's a strong argument for a summer sitting.

I understand there are technical steps to be taken, but I've taken confidence from the comments of the Speaker and others. It seems as though the House administration has adapted very quickly. I would expect those actors to sound a strong note of caution if they didn't feel confident they could deliver remote divisions, because if it all went haywire, they'd be the ones blamed.

So I would like to see even faster progress than that. I think it's important that Parliament make up for lost time and start to move a broad agenda of parliamentary business forward in order to keep up with history, which is moving very quickly right now, and to resume the issues that were important.

[*Translation*]

**Ms. Christine Normandin:** Thank you very much.

I have a question for you, Mr. Roberge. We have discussed various voting systems and the importance of a vote where the individual can be seen. However, recorded division can take a very long time, especially if a vote on a number of issues is required. Since a very short time is available for voting, as well, a problem may arise if a technical issue occurs when it's our turn to vote.

I would like to hear your thoughts on a possible electronic system that enables one to vote yes or no and includes a video recording where the person says they vote yes on one bill, but no on another. That information would be sent by email, and then validated. That would give us more time to vote and to validate the vote twice. Would that be a worthwhile option to analyze?

• (1150)

**Mr. Pierre Roberge:** Yes, Ms. Normandin, that sounds good to me. As I was saying in my opening remarks, redundancy is likely the most important aspect of vote reliability, as is the flexibility you have in voting.

What is more, I think you have applications that use authentication mechanisms. The House of Commons technical team is very competent, and I have faith in it. When given a problem to solve, it generally has the resources it needs to achieve good results.

**Ms. Christine Normandin:** So it would be worthwhile to point out that we can set the parameters of that kind of a system instead of choosing a pre-established system.

**Mr. Pierre Roberge:** Yes. As Mr. Morden was saying, it is a matter of flexibility. We have to act quickly to remain efficient and hold parliamentary meetings. What is important is that nothing prevents us from making adjustments after the initial implementation.

**Ms. Christine Normandin:** That's excellent.

My next question is probably intended more for professors Essex and Goodman, but I invite all the witnesses to use the opportunity and answer it.

If we implemented a remote voting system, would you recommend that even members present in the House use that system or for us to be able to vote in both ways at the same time? What would be ideal?

[*English*]

**Mr. Aleksander Essex:** Thank you. I'll try to tackle this question.

There is strength in simplicity, especially when we're talking about cybersecurity and technology.

One of the reasons Dr. Goodman and I have gravitated more towards video voting as an approach is that it does have a certain simplicity to it. It's a lot easier to match a person's face and a voice—deepfakes notwithstanding—whereas when you are voting through an app, what the system is recording is not that you voted, but rather that somebody with your credentials voted. This is exactly what we saw in the Ontario municipal election. People were receiving PINs for their children who were in university, spouses were voting on behalf of each other, and so forth.

Video voting does provide a nice way to see the authenticity of the person there, subject to a number of other questions involving some of the issues discussed, but whatever you gravitate towards, I would encourage you to look for an elegant and simple option.

[*Translation*]

**Ms. Christine Normandin:** I will clarify my question. If some members were using an electronic system to vote remotely while other members were present in the House, should everyone use that electronic system to vote or could we have a remote electronic vote at the same time as a physical vote in the House?

[*English*]

**Mr. Aleksander Essex:** If I could borrow a line from the chair, whom I have been watching during these committee proceedings, I suppose that would be for the members to decide for themselves.

I can tell you that in the Ontario municipal election we saw this sort of hybrid model in many Ontario cities. Some people would go to an in-person place to cast a paper ballot, some people would vote online and some people would vote via the telephone.

**The Chair:** Thank you, Dr. Essex.

Next is Ms. Blaney for six minutes, please.

**Ms. Rachel Blaney (North Island—Powell River, NDP):** Good morning, and thank you all so much for your testimony today.

The first question I have is about voting. First of all, just for the record, I agree that if we're going to do some sort of virtual voting, I would much rather see someone's face on the screen voting one way or another. I think it would allow us all to have that high level of accountability.

As a parliamentarian who is farther away from Ottawa, I also really respect the fact that being able to choose the health of yourself, your loved ones and your constituency is also a priority at this time. I agree that the hybrid model is a good step forward.

One of the challenges we've heard about, though, is how many decisions are actually made in the House through voice voting.

Maybe I can start with you, Ms. Goodman, if you have any information or thoughts on how to do a voice vote during this time.

• (1155)

**Ms. Nicole Goodman:** A voice vote? You mean online.

**Ms. Rachel Blaney:** Yes, with the hybrid model.

**Ms. Nicole Goodman:** I have some hesitations about the hybrid model based on what I've seen. I think we want to be careful. I definitely see the value in it and I know that other jurisdictions around the world are adopting it. I'd like to watch how that plays out.

I think we have to be careful to make sure that we're not creating two tiers here, where some MPs have better access, for example, if it's not just a vote but also debate, including some in-person debate in the legislature and some debate online. We need to be sure we're not creating two tiers of classes here, but that all MPs have equal access to speak and to ensure representation.

With respect to the voice vote specifically, I think it depends on the nature of the vote, but as I understand it, when you call a vote, there would be the yeas and the nays.

**Ms. Rachel Blaney:** Yes, and usually they're in the same room, so you can measure the loudness and that let's you know which way we're going.

**Ms. Nicole Goodman:** You could have a system where you could go through the yeas first, then the nays. Everyone who is voting yea would raise their hands and you would go through them and count them; and then you could have the nays and go through and count them. This is really where I think it speaks to the importance of also double-checking and having more than one actor verifying the vote.

**Ms. Rachel Blaney:** One of the other challenges, of course, is that as we're in this model we have different challenges facing all members given the realities of their lives. One of the things we've had several folks talk about is predictability, so that we know when we're voting.

Maybe I could start with Mr. Morden. Perhaps you could speak to the inclusiveness of having predictable times for voting.

**Mr. Michael Morden:** I think that's important. In fact, I think that's also a discussion for the in-person Parliament when it resumes. It's incumbent on government to adapt its approach to how it wants to manage parliamentary business in order not to exploit this adaptation to alter the power balance or to acquire greater control over parliamentary business.

I don't have a technical fix for that. It's something that deserves scrutiny and certainly something that should be provided to the limited extent we're able to, but I think it's an important caution and something that this committee could reasonably seek assurances from the government on.

**Ms. Rachel Blaney:** Mr. Essex, do you have anything to add on predictability around voting times?

**Mr. Aleksander Essex:** I will approach this question from my experience in general elections. Predictability is right at the core of the democratic principles that you might have for an election, and the predictability would feed into the notion of fairness and that everyone has an opportunity to vote.

Unpredictability has, of course, very detrimental consequences to the democratic process. One example from the other day was the curfew in Washington, D.C. at the same time as people were voting, so there was interference there between the police curfew and the actual voting. There was some exemption given to voters, but then law enforcement wasn't quite adhering to that, so it created a very unpredictable environment. Of course, that's deeply concerning.

Yes, predictability in votes, whether they're in a general or legislative context, is an absolute must.

**Ms. Rachel Blaney:** My final question is for Mr. Roberge. One thing that you talked about in terms of our security is the importance of creating those relationships and collegiality. I'm wondering if you could speak to that. I know that one of the biggest challenges for all of us is that we're not in the same space in the same way that we usually are, which is where we build relationships across party lines. I also think it's important to connect that personal connectedness with our ability to manage security.

• (1200)

**Mr. Pierre Roberge:** Having been running a decentralized business for 10 years, I know that we need to meet as often as possible as a whole team to build up that collegiality.

In the case of Parliament, what I see you needing to do to avoid future big problems.... I don't think it's a problem at the moment, but there are subtle attacks that could be made. For example, someone could lower the quality of video and connectivity of people temporarily when they're actively debating until it frustrates them and they disconnect. There are very subtle and different levels of attacks that we will be facing in the future.

**The Chair:** Thank you, Mr. Roberge.

Next up is Mr. Brassard for five minutes, please.

**Mr. John Brassard (Barrie—Innisfil, CPC):** Thank you, Madam Chair.

Thank you to all the witnesses.

Dr. Goodman, you talked about the potential of flexibility and accessibility. On the one hand, you said that you agree that during a crisis it's a good mechanism to move to remote voting. The Constitution dictates that Ottawa is the seat of Parliament, so there are some challenges. You mentioned as well circumstances where an MP may have busy constituency schedules, the issue of maternity leave and the other examples you gave.

However, there are circumstances where members, for example, could use that as a reason not to be in Ottawa, and there may be situations where they do have a busy constituency schedule and need to be back in their ridings and not come to Ottawa. It could happen when there's a close election and they don't want to be in Ottawa, and they would use remote voting as a mechanism to not be back in Ottawa. There could be situations where an MP is facing, for exam-

ple, very serious criminal charges and doesn't want to face the scrutiny of the parliamentary press gallery.

How would you propose to differentiate between what would be, as you said, those convenient situations and the other types of situations I mentioned that have MPs avoiding being in Ottawa?

**Ms. Nicole Goodman:** Thank you very much, MP Brassard, for allowing me the opportunity to clarify.

With respect to the birth of a new child, there's precedent there in other legislatures with proxy voting, and there's a good argument to be made there for extending that to electronic voting.

With respect to individual MPs, I wasn't necessarily thinking of busy schedules, I was thinking more of crises. For example, say there were some kind of flood in an MP's community and that MP needed to be there, or there was a big fire or some other kind of crisis. With COVID now we think of ourselves as having a macro-crisis, but I'm thinking of a micro-crisis in a constituency, "micro" being small because it affects a particular area. That could be very well defined so that it wouldn't be taken advantage of.

With respect to sickness, no example comes to mind right now, but I have seen or heard of situations where a member was battling cancer and either wasn't able to attend a vote, to participate, or some members have come while they are very ill to vote just once. In cases of sickness like that, the member could stay in the hospital or at home and rest and be able to participate. I'm thinking of extenuating circumstances, not just busy schedules.

**Mr. John Brassard:** Thank you for that clarification.

The other question I'd like to ask is of Mr. Roberge.

Some of the existing mechanisms that we have include, for example, pairing of MP voting, and there's the potential for proxy voting and for applied votes.

On the issue of hardware and software, what would be necessary to ensure the integrity of remote voting, and what financial costs would we be looking at, other than the normal mechanisms that exist, to develop or create that type of technology?

**Mr. Pierre Roberge:** Thank you. That's a good question.

With regard to the costs, I will go in reverse order. They could be kept to a minimum if we played the cards of redundancy, where we have two or three voting mechanisms and make sure that a vote makes it through and is reliable. That way we could use a less costly solution.

In Eastern European countries, they have SIM cards in their cell phones they use for signing transactions and documents, or things like that. They're effectively really cheap, and the cost of implementation is relatively cheap as well.

Technologically, for voting, it's fairly inexpensive to implement and very efficient.

• (1205)

**Mr. John Brassard:** My next question is for Mr. Morden.

Mr. Morden, you talked about radical adaptation in radical times. I think that's what you said in your presentation. We can all agree that these are not normal times.

We heard in earlier evidence—and perhaps you followed this from Great Britain—that the time to look at these types of changes is not at the height of a crisis but afterwards. Would you agree that the right time to look at the potential changes Parliament could enact to deal with future crises is when we're in normal circumstances?

**The Chair:** Unfortunately, that's all the time we have.

Mr. Morden, can you answer that with a yes or no?

**Mr. Michael Morden:** I'm not sure. I guess the answer is no.

**The Chair:** Next we have Dr. Duncan.

**Hon. Kirsty Duncan (Etobicoke North, Lib.):** Thank you, Madam Chair.

Good morning to all of our witnesses. Thank you for coming and for your tremendous expertise.

I'll start by saying that democracy does not have to stop in the face of a crisis. We can rise to this challenge. We can evolve during this unprecedented time, and I think we have been evolving.

I have a limited amount of time for questions, so for the first few questions I'm going to be looking for yes-or-no answers. I'll begin with Mr. Morden, if I may.

Mr. Morden, do you believe it's possible for members of Parliament to regularly attend Parliament in person right now, with the travel restrictions, health vulnerability and concerns that their returning home from Ottawa will expose constituents in vulnerable areas? I'd like a yes or no, please.

**Mr. Michael Morden:** No.

**Hon. Kirsty Duncan:** Mr. Morden, do you believe that all members should be empowered through remote voting, yes or no?

**Mr. Michael Morden:** Yes.

**Hon. Kirsty Duncan:** I'll turn to Dr. Essex, if I may.

Dr. Essex, did you and Dr. Goodman argue in Policy Options on March 25 that online voting is “entirely possible for MPs”? I'd like a yes or no, please.

**Mr. Aleksander Essex:** I believe that was in the title of the article, so yes.

**Hon. Kirsty Duncan:** Dr. Essex, did you write in the same article that “Parliamentary voting...is entirely workable from a cybersecurity perspective”, yes or no?

**Mr. Aleksander Essex:** Under the right conditions and with careful design, yes.

**Hon. Kirsty Duncan:** Dr. Goodman, you've spoken about this today. Did you write that it is possible to verify an MP's vote online?

**Ms. Nicole Goodman:** Yes, with the right security software.

**Hon. Kirsty Duncan:** Dr. Goodman, did you write that “the federal government has the resources to provide MPs with the necessary cybersecurity infrastructure to ensure the protection of electronic information”? Again, I'd like a yes or no, please.

**Ms. Nicole Goodman:** Yes, with outside consultation with experts who have done this before.

**Hon. Kirsty Duncan:** Dr. Goodman, did you write that “the government has the capacity to provide MPs training on procedures necessary to ensure votes are successfully entered into the record”, yes or no?

**Ms. Nicole Goodman:** Yes.

**Hon. Kirsty Duncan:** Dr. Goodman, do you advocate for an on-line voting system premised on MPs' verifying their vote selections, yes or no?

• (1210)

**Ms. Nicole Goodman:** Upon reflection, I think video voting would work best, so I would put in verification to double verify parties within the legislature.

**Hon. Kirsty Duncan:** That's helpful. Thank you.

Dr. Goodman, do you advocate for “secure infrastructure that includes a government secured device, application and network connection”?

**Ms. Nicole Goodman:** Yes. That would be more for application- or web-based voting, but obviously we would need infrastructure to facilitate the video voting.

**Hon. Kirsty Duncan:** Dr. Goodman, you talked about the positives of video voting. What positives might there be for application- or web-based voting?

**Ms. Nicole Goodman:** I think Dr. Essex might be good to chime in here, but I know that with the web-based and application-based, for example, it's easier to capture intent. It can be clearer, but there are other issues. I think in terms of security it would be email at the bottom, then web-based and application-based, but I think Dr. Essex should probably speak to that.

**Hon. Kirsty Duncan:** Thank you.

You've talked about the positives for video voting. I'd like to hear what the positives are for web or application. You talked about four methods.

**Ms. Nicole Goodman:** Yes. The big positive for application and web is I think intent. Also, they can be very user-friendly. It depends on how they're designed. They work very well. In Estonia, for example, and Switzerland, they have worked well, but there are additional cybersecurity challenges.

**Hon. Kirsty Duncan:** I think that's my time, Madam Chair.

**The Chair:** That's your time. Yes.

**Hon. Kirsty Duncan:** Thank you to the witnesses.

**The Chair:** Thank you for monitoring that.

You have five minutes, Mr. Doherty.

**Mr. Todd Doherty (Cariboo—Prince George, CPC):** I'll give my time to Mr. Reid, please.

**The Chair:** Absolutely.

Mr. Reid, you have five minutes of questioning.

**Mr. Scott Reid (Lanark—Frontenac—Kingston, CPC):** Thank you very much. I have a little timer here that I'm going to start so I don't run over.

Thank you to my colleague Mr. Doherty for being so gracious and letting me have this time.

I want to start with a separate question relating to proxy voting. I haven't heard anybody speaking in favour of it. I wonder if we could just go around to the witnesses.

Maybe you can just quickly signal whether you are opposed to proxy voting or in favour of it. I'm not sure who to start with.

Why don't we start with you, Ms. Goodman, seeing as you're the person at the top of my screen?

**Ms. Nicole Goodman:** I'm not opposed to proxy voting. However, after some consideration, and reviewing remote electronic voting and proxy voting, I do feel that the remote electronic voting enables representation and inclusiveness more fully.

**Mr. Scott Reid:** Dr. Essex.

**Mr. Aleksander Essex:** Proxy voting in a general election has a lot of problems. I know that they allowed it in Toronto and there were instances of abuse. I don't think that would be as easy to abuse in a legislative context where the voting would sort of be in many cases along party lines—

**Mr. Scott Reid:** I'm sorry to interrupt there, and thank you for that, but what you've just said does imply that the MP is simply a functionary of the party and not someone who might vote independently. That's effectively what you've just asserted.

Look, I was setting you guys up. Here's the question I wanted to ask. Isn't it the case that we deal with—

**Mr. Aleksander Essex:** Well, I—

**Mr. Scott Reid:** I'm sorry, Mr. Essex. I'll ask you to come back in a second.

That's a concern I have. A second concern is, what about votes that occur without advance notice so that the MP cannot, even in theory, express their views to the proxy voter who's voting on their behalf?

I'm sorry, Mr. Essex. Now you can carry on with your response. Thank you.

**Mr. Aleksander Essex:** I'm not implying that an MP is a function of a party. I'm a cybersecurity expert. I am aware of the notion of a whipped vote, which in that case would imply that there would be a sort of an understanding ahead of time on how members would

vote, but setting that aside, in proxy voting, there of course would need to be time for a member to communicate their intention to their proxy.

**Mr. Scott Reid:** Fair enough, Mr. Essex, and thank you. Forgive me for posing something that's outside your area of expertise. You just happened to raise the point that got me going.

Mr. Morden, can I go to you for this?

• (1215)

**Mr. Michael Morden:** Thank you so much for the question. I think I share your concern, if I understand it, in that we see MPs as individuals and as unique representatives of their communities. We prefer a model like a virtual roll call, in which there is that moment of accountability when the members themselves visibly commit their vote.

**Mr. Scott Reid:** Thank you.

Finally, I think we have only one more witness. Is that right, Mr. Roberge?

**Mr. Pierre Roberge:** That's right. Yes.

From a technical point of view, I don't have a problem with it. I think it's more of a function problem, as the others have outlined.

**Mr. Scott Reid:** Okay. Thank you.

I wanted to turn to the issue of voting online. I assume that it would essentially have to be a roll call. We'd go through one at a time, essentially replicating what we do in the House of Commons. Would that be correct?

**Mr. Aleksander Essex:** Who's the question addressed to?

**Mr. Scott Reid:** I'm not sure. It's for someone who has the right kind of expertise to determine from a technical point of view what is meant by online voting, as opposed to app-based voting.

**Mr. Aleksander Essex:** We're distinguishing between a vote that might be input via a web-based interface using a browser, in which you sign in on a laptop or a computer, versus an application that might be on a smartphone. The network connection and security and so forth are managed slightly differently—the credentials and all of that sort of stuff. There are subtle differences I could tell you all about if you're interested, but—

**Mr. Scott Reid:** No. We only have 30 seconds here.

I just want to ask this question. How do we deal with someone who is dropped during a vote? Is there some way of getting them back in the voting so they can express their preference? Is there some way of catching the fact that they were not trying to abstain but rather were lost partway through the vote?

You can see the technical issue I'm worried about. This can be relevant. There have been governments.... The fall of the government was once decided by one vote while I was an MP, so you want to get these things right.

**Mr. Aleksander Essex:** Yes, absolutely, and I certainly remember that time with those close votes.

The issue that you're raising about bandwidth and dropping is actually a bit of a concern, especially if there is a threat actor who has the capability of cause the member's vote to drop at a specific time.

**The Chair:** That's all the time we have. I was waiting for a good point to cut there.

**Mr. Scott Reid:** Thank you to the witness, and thank you too, Ms. Sahota.

**The Chair:** Mr. Gerretsen.

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

I'll just start by saying that I'm extremely glad to see that some of the witnesses, if not all, have mentioned the fact that this committee has been approaching this as a temporary issue. I think it's safe to say that all members of this committee would rather be meeting in Ottawa and voting in Ottawa, but the reality of the situation is that we are in uncertain times that require us to look for alternatives. I am unaware of any member who would like to implement this stuff on a permanent basis.

Dr. Goodwin, or is it Ms. Goodwin?

**Ms. Nicole Goodman:** Just Goodman.

**Mr. Mark Gerretsen:** Goodman, but is it Dr. or Ms.?

**Ms. Nicole Goodman:** I have a Ph.D., but either is fine.

**Mr. Mark Gerretsen:** No, I want to get that right.

Dr. Goodman, you seem to be reluctant to do anything that is web-based or application based. I really want to understand that a little bit better.

Mr. Essex talked about an example in Sarnia where there was an error with the difference between “agree” and “disagree”. That might work if you have a city council of 15 or 20 people, where you can catch that easily, but the reality of the situation is that...

You'd have to talk me through how you do a voice vote in a parliament of 338 people, which, in our traditional sense, works through the parties. If it's a government piece of legislation, all government members would vote. Then, in succession, any other parties' members would vote. How do you line that up in the Zoom system so that you have everybody in the line? How does that work when we have 17-20 pages of thumbnails of videos? Are they just literally jumping back and forth all over the place?

How do you implement that practically speaking?

**Ms. Nicole Goodman:** It's a great question. Thank you.

You could go by party. You could go alphabetically. You—

• (1220)

**Mr. Mark Gerretsen:** Right. I'm sorry to interrupt, but we're not going to be lined up on the screen like that, so that if we were to go alphabetically, then we'd be jumping back and forth on Zoom from screen to screen. The way Zoom works is that if you interrupt me right now and just say, “I agree,” the screen won't actually show you as the main image until you've been talking for a few minutes,

so I think there are a lot of technical issues that need to be addressed within the Zoom platform to make a voice vote actually work. Would you agree at least that there are some challenges?

**Ms. Nicole Goodman:** Absolutely, I would agree that there are challenges. Just between the voice vote and the show of hands, I am more supportive of the show of hands, but I'd just like to make a quick point on the web and application-based voting.

**Mr. Mark Gerretsen:** Okay. I'll let you get to that because I want to ask you a question about it.

Dr. Essex referred to “deepfakes notwithstanding”. I think we need to talk about deepfakes. I don't think we can say “deepfakes notwithstanding” and put that off to the side because I think it is something that is a reality and that can become even more of a reality for someone to actually implement.

Here's my own personal opinion when we're talking about authentication. With this device, I go to Tim Hortons down the street. I tap the side, and my wallet opens. It won't let me tap the device to pay until it gets my retina and does a facial recognition of me. Would you not agree that the technology that's built into smartphones would be so much more secure in identifying somebody than using or relying on somebody to say, “I agree” or “I disagree”, or “yea” or “nay”?

Dr. Goodman or Dr. Essex.

**Ms. Nicole Goodman:** To comment very quickly on web- versus application-based voting, it's not that I'm opposed to those options. I recognize that for the U.K. House of Commons, they built this voting app software—

**Mr. Mark Gerretsen:** I just need to understand—I'm running out of time here—which one you think is more secure, which one has the ability to have more security. Is it the voice vote with the image, or is it the authentication software that's built into these devices?

**Ms. Nicole Goodman:** I can't give a blanket answer to that, because—

**Mr. Mark Gerretsen:** Mr. Roberge, do you have an answer for that, being the security expert?

**Mr. Pierre Roberge:** Definitely, at the moment, I would use video and voice over apps.

**Mr. Mark Gerretsen:** Okay.

I'll tell you how I picture it. You are authenticated. You are asked how you want to vote. Then you confirm how you want to vote, which is all how the U.K. does it. The final step would be an email sent to you saying “this is how you voted”.

Would that be a secure way of doing it?

**Mr. Aleksander Essex:** No.

**Mr. Mark Gerretsen:** It would not? Why?

**Mr. Aleksander Essex:** Email is not encrypted end to end.

**Mr. Mark Gerretsen:** No, no, the email is just an email confirmation of how you voted. It's just to let you know. That's your secondary step that you guys talked about—

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

Next up is Madame Normandin.

[*Translation*]

**Ms. Christine Normandin:** Thank you, Madam Chair.

Professor Essex, you said earlier that it is important to have a way to recognize when things go awry, but it is even more important to put that into practice.

Before the result of the vote is announced, the IT or security service could deliver a certificate stating that no technical problem occurred and there was no cyber attack. Only once that has been done would the result of the vote be revealed.

Would that be a good idea?

[*English*]

**Mr. Aleksander Essex:** There are a number of ways you could go about it. These would be procedural matters. The core procedure that needs to be in place is something to handle both, (a), when somebody doesn't have an opportunity to vote because of some kind of network issue, such as when the website goes down and you need to be able to recover from it; and (b), if it is detected that a member's vote was changed by accident, error, or otherwise. There needs to be a method to recover from both of those.

It certainly seems that you may want to have at least some kind of tiered or staged announcement of the vote outcome, a sort of preliminary and then final vote. You can be optimistic about it and announce a preliminary result, subject to the CSE or whatever. IT security might want to apply to it afterwards.

• (1225)

[*Translation*]

**Ms. Christine Normandin:** Mr. Roberge, can a security certificate be obtained quickly?

**Mr. Pierre Roberge:** Who would be issuing that certificate?

I am not sure I understand.

**Ms. Christine Normandin:** It could be provided by the House technical team. The certificate would state that no issue or cyber attack occurred during the vote.

**Mr. Pierre Roberge:** I don't think such a certificate exists. However, we can have a measure of certainty.

**Ms. Christine Normandin:** Mr. Morden, do you think it is important to have some time between the vote announcement and the vote itself for members to be able to come together and discuss? A vote is never black or white. It is important to give whips time in the democratic process.

[*English*]

**The Chair:** You have 10 seconds.

**Mr. Michael Morden:** I think time and predictability should be primary, first-order principles of a virtual parliament.

**The Chair:** Thank you.

Ms. Blaney, please.

**Ms. Rachel Blaney:** Dr. Essex, you were going to answer Mr. Gerretsen's question earlier. I'm really curious to hear your response.

**Mr. Aleksander Essex:** May I ask which question of the many I was asked?

**Ms. Rachel Blaney:** It was just at the end, when he talked about the process that he saw. He outlined the email verification. You said there were concerns about that. I'm just wondering if you could clarify what those concerns would be.

**Mr. Aleksander Essex:** Those were concerns about email verification.

**Ms. Rachel Blaney:** For the vote.

**Mr. Aleksander Essex:** Well, there has to be some avenue to verify or identify that a vote was correctly recorded. That could be via a website or some other channel. The issue we have with email is that it's not encrypted end to end. It's not a suitable technology for this purpose.

**Ms. Rachel Blaney:** Thank you.

Mr. Roberge, you were asked a question about what method is the best—I'm going back to Mr. Gerretsen's question again—but what is the best method for transparency in voting? You said on the screen, yea or nay.

Can you speak about why that is the most secure, and any concerns you may have about using a smartphone, for example, to vote in Parliament.

**Mr. Pierre Roberge:** To clarify Mr. Gerretsen's question, he was asking if the way the U.K. Parliament is doing it at the moment is pretty good. I find the way he described it—I'm not familiar with it—sounded good where you vote by video, and then there's validation through email. That's what I understood.

That sounds like a pretty decent and probably one of the best and easiest implementations we can do at the moment.

The reason is that even though deepfake is on the table, it's still one of the hardest attacks to pull off at the moment versus attacks on applications or some data in the database. Those are two different worlds of attacks. That's why I think voting with video confirmation, and then confirming with another method, either email or application, has high value.

**Ms. Rachel Blaney:** Thank you.

I believe that's my time.

**The Chair:** Thank you, Ms. Blaney.

Thank you to all of our witnesses today. We have heard very insightful information from the professors and both of the organizations that have come before us today. We are very grateful.

I think this panel has got us down to the core of what we are trying to study, so it was extremely helpful for us in putting together the report.



We will take about five minutes or so to clear these witnesses, and then bring in our new witnesses, and do some checks for them.

• (1225)

(Pause)

• (1235)

**The Chair:** Welcome back. We're going to get started. I would just like to ensure that everyone is in the gallery view at the top right-hand corner. You can switch between speaker view and gallery view. We'd prefer if you stayed on gallery view so you can see all of the members in the committee meeting.

I'd like to make a few comments for the benefit of the new witnesses before us.

Before speaking, please wait until I recognize you by name. When you are ready to speak, you can click on the microphone icon to activate your mike. Please let us know if you're not familiar with the Zoom application, and we can walk you through some of the features.

I remind everyone that all comments should be addressed through the chair.

Interpretation works just as it does in a regular meeting, if you have appeared before a committee before. You'll have a choice at the bottom of your screen of floor, English or French. As you are speaking, please select the language you are speaking in.

We have simultaneous interpretation. Please make sure, in order to make the lives of the interpreters a little bit easier, that you're speaking slowly and clearly and that you have the right language selected at the bottom of your screen.

Also, please ensure that your mike is on mute when you are not speaking. For quicker interactions later on, when we get to the question-and-answer portion of the panel, you can use your space bar to unmute your mike. Pressing down on the space bar unmutes the mike temporarily. That would be for quicker interactions. However, for your opening statements, I would suggest that you unmute using the icon.

I think you've all been told about headsets. They do improve the quality of the sound, especially for the interpreters, who have to concentrate quite a bit in order to provide the interpretation, so if you have a headset, please wear it.

I'd like to welcome the witnesses before us today. We have academics, and it's really great. Even in the previous panel we got a lot of valuable information from the professors who came before us.

We have Mr. Ghorbani, professor and director at the Canadian Institute of Cybersecurity, University of New Brunswick. We have Mr. Jourdan, professor of computer science, faculty of engineering, University of Ottawa. We have Chris Vickery, director of cyber risk research at Upguard.

Welcome, everyone. Thank you so much for being here today.

We'll have seven-minute opening statements from each of the witnesses, starting with Dr. Ghorbani.

Go ahead, please.

• (1240)

**Mr. Ali Ghorbani (Professor and Director, Canadian Institute for Cybersecurity, University of New Brunswick, As an Individual):** Honourable members of the Standing Committee on Procedure and House Affairs, thank you for inviting the Canadian Institute for Cybersecurity at the University of New Brunswick to speak today about cybersecurity considerations relating to the establishment of a hybrid Parliament.

My name is Ali Ghorbani. I am a professor of computer science, a tier one Canada research chair in cybersecurity, and the founder and director of the Canadian Institute for Cybersecurity.

Cybersecurity and privacy, once issues only for technology experts, have become widespread concerns in business and society. Cybersecurity is no longer just an IT problem; it's a business problem; it's everyone's problem. The weakest link in cybersecurity is now people, not devices. Here at the Canadian Institute for Cybersecurity, we think that the human factor is considered the biggest threat to cybersafety, and we strongly believe that cybersecurity requires multidisciplinary and human-centric solutions.

The Canadian Institute for Cybersecurity is one of the first institutions to bring together researchers from across the academic spectrum to share innovative ideas and carry out groundbreaking research into the most pressing cybersecurity challenges of our time. We have been doing research and development and entrepreneurial activities in this area non-stop for over two decades. We have developed multiple practical network security solutions, and our research has led to the establishment of several companies. Currently, the institute has a team of 60 researchers, technical staff and graduate students, and a state-of-the-art architecture and infrastructure.

The science of cybersecurity is about managing risks and avoiding surprises. There will be security risks with any online communication platform. In the "Virtual Chamber" report of May 7, 2020, it is written:

Members who wish to participate remotely will connect using a videoconferencing platform integrated into existing on-premise technologies.

Let me briefly highlight the security and privacy issues in relation to the proposed platform from two perspectives: users and organizers.

On the user side, the first issue is awareness of cybersecurity. The remote participants who use the platform for virtual sittings must be aware of the security risks associated with the use of online video conferencing platforms or, if not, must be trained for such. The goal is to avoid issues such as installing platform software from an unofficial site, which can be malware; phishing scams asking to join video conferences, which steal credentials; and overprivileged video conferencing application by using the web version, which sits in a sandbox in the browser when possible, instead of installing an application.

The second issue is technical issues for remote access. The remote participants who use the platform for virtual sittings must have satisfactory assets for remote access or, if not, must be provided with such. The goal is to avoid issues such as hardware shutdown during connection due to power outage, which can be considered as an availability issue; slow connection and breaking during meeting, which can be considered as an availability and/or integrity issue; and vulnerable webcams, which can be accessed by unauthorized users and can be considered as confidentiality and privacy issues.

On the organizer side, the first issue is trusted computing based on trusted hardware. With regard to the proposed integration of a multimedia system with video conferencing and a voting system, it is known that a system is as secure as its weakest link.

Furthermore, computing hardware has security issues, such as branch direction prediction attacked by Spectre.variant 1. Therefore, it raises the need to use trusted hardware such as trusted platform module, TPM, also known as ISO/IEC 11889, which is a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.

• (1245)

The second issue is verifiable software. The software integrated in the virtual chamber must be verified, or if not, it must be open sourced, such as Helios for online elections system, or openly reviewed such as a Zoom proposal for end-to-end encryption for video conferencing.

The goal is to avoid software vulnerabilities, such as meeting bombing when an unauthorized person joins a meeting; client application chat issues, malicious links and arbitrary file write; and security risks related to operating systems of the video conferencing platform and user management system.

Last but not least, the third issue is secure cloud and networking technologies. The network integrated to the virtual chamber must be private, or if not, it must be secured. The goal is to avoid cloud and network vulnerabilities, such as security risks related to streaming video, such as stream grabbing and uploading; and security risks related to data routing, such as route manipulation and route hijacking, which requires that the integrated platform must offer the ability to choose through which region of the world their data would be routed.

With that, thank you again for inviting me to be with you today. I look forward to your questions.

**The Chair:** Thank you, Dr. Ghorbani.

Next we have Mr. Jourdan.

[*Translation*]

**Mr. Guy-Vincent Jourdan (Professor of Computer Science, Faculty of Engineering, University of Ottawa, As an Individual):** Madam Chair, ladies and gentlemen members of the committee, thank you for inviting me to appear before you.

My name is Guy-Vincent Jourdan. I am a professor of computer science at the University of Ottawa's Faculty of Engineering. My research topics include software security and cybersecurity. Over the past few years, I have worked specifically on cybercrime and cybersecurity, in collaboration with IBM.

Is there a reasonably secure way to implement a hybrid Parliament in Canada, including a remote electronic voting system based on the report produced in May here titled "Virtual Sittings of the House of Commons"? I think so, as long as we are given the means to do so.

Of course, it is difficult to be very specific without an in-depth preliminary study whose conclusions would not fit into seven minutes anyway, but here are a few important points, in my opinion.

Concerning parliamentary discussions and debates, a number of key elements facilitate the process. First, our Parliament has an existing and effective security structure, recognized as such, and competent staff we can count on. Secure communications among members, secure infrastructure, control of devices used remotely and the software installed on those devices have all existed for a long time.

In addition, the situation we are facing is global and the needs are similar everywhere else. For example, I know that Brazil, Spain, the United Kingdom, Wales and the European Parliament have all set up forms of virtual Parliament, some with a remote electronic vote. So it is feasible, and we can, therefore, also benefit from the feedback and lessons learned around the world.

The idea of virtual sittings and remote votes may be relatively new for many parliaments and governments, but we shouldn't forget that those systems have been used for a long time in the private sector to handle daily business, organize confidential meetings and boards of directors or to vote at shareholder meetings.

Video conference software, in particular, has been the subject of security analyses for a long time. For instance, the NSA recently published and has been updating a document containing the important points on selecting and using that software, such as end-to-end encryption, multifactor authentication or the use of certified and controlled devices.

In that report, a number of solutions are positively assessed, such as the solutions provided by Microsoft or Cisco, or the Zoom software, which we are using now.

However, there is more to the issue than choosing a video conferencing software. Parliament certainly needs to be able to debate, but it also needs to be able to call for a vote, vote and have confidence in the result of the vote. It must be possible to respect the rules and adapt them as needed.

The Internet vote is an issue in itself. I think that we can generally say that the IT security community is not favourable to it, as the challenges are too great, the risks too high and the benefits dubious. That said, once again, we have to look at what we are talking about. The parliamentary vote is not the same thing as the Internet vote in general.

One of the fundamental differences, first and foremost, is that it is a public ballot, which, of course, considerably facilitates the problem resolution. The result can be widely disseminated, and everyone can know how the votes were counted.

Moreover, the electorate is very small, and every member is known. The devices used for the vote are controlled and managed by the parliamentary technical staff. Members can also be provided with tailored training and support. Finally, the benefit of such a vote seems clear, at least right now.

We can imagine that the system will be a combination of an accredited video conferencing system, a secure communication system and a voting system, possibly integrated into one of the two systems, but not necessarily.

- (1250)

During normal proceedings, the member will be asked to vote through a secure communications system. During the vote, a biometric authentication will take place, and a number of receipt orders will be published immediately. Procedures will have to be implemented to manage abnormal situations, such as connectivity losses and handling errors.

To maximize the likelihood of success, it must first be ensured that the devices used are managed and controlled by the technical team, as well as verified, certified, updated, secured, and so on. As far as I understand, that is already the case.

Next, it must be ensured that the software used comes from a certified supply chain, that it has been verified by independent teams and continues to be verified regularly, that it has adequate certifications—such as FIPS-140—and that it is kept up to date. Once again, my understanding is that this is also currently the case.

The system will need to be integrated into the existing parliamentary infrastructure: multifactor authentication mechanisms, a virtual private network, cloud architecture, and so on.

What is more, registries will have to be produced and maintained in a secure manner at every possible level to be able to respond to and remedy any real or perceived issues. Clear and effective procedures will have to be implemented to define the steps to follow in case of problems and to ensure that the sitting can continue.

Finally, the proposed solution will have to be reviewed and critiqued regularly by independent specialists from the private and academic sectors. Ideally, the solution will be made public.

None of this seems out of reach to me.

Thank you.

[*English*]

**The Chair:** Thank you.

Mr. Vickery.

**Mr. Chris Vickery (Director of Cyber Risk Research, Up-Guard, As an Individual):** Hello, and thank you for inviting me to provide my thoughts and to answer questions on this very important and very interesting time we are in.

The solution that I have worked out, I believe, is minimal on effort required and maximal on trust. I think that with a parliament-style vote where there are only a few hundred people, it is definitely possible to be absolutely confident in the result that is shown, and here is how you do it.

I am not in favour of web-app-based solutions, video voting, or things that require a phone display, primarily because those things can be programmed to lie and display things that are not true to both sides. It's just something that is not going to be overcome any time soon. Even if the implementation is secure and safe, the fact is people who use their phones for other things are going to be continually taken advantage of in the general public, and we're going to see report after report in the general sense about phones being insecure. That will degrade the integrity of these official votes that are being done through phones, even if they're being done in a secure way. That is something that is also not going to be overcome.

What I would suggest as a solution involves a separate physical piece of hardware that is plugged in and requires no training whatsoever. I have an example of one right here. You plug it in with the regular ethernet to any member's home, whatever, and it is set with software that already exists to transmit but not receive.

The benefits of this are that an adversary would have to know the precise window of time that the vote is happening. They would have to compromise the ISP transmission. They would have to have the decryption capability already figured out and the preloaded key known in advance. They would have to be able to change or modify the packet that is sent instantaneously. That can be checked, because there are time stamps on the transmissions. You calculate how long it took for a transmission to go from a member's location to the official place of the vote being received. Through math, logic and physics, we can figure out if it was physically possible that it made it that quickly or if that transmission was unreasonably slow, which would suggest that it had been intercepted and modified, repackaged and sent. You can get an average heartbeat signal going, and as long as it arrives within that specific time frame and reasonability, you can be fairly sure of the result.

The important other factor is a secondary outside band confirmation. I would suggest that you then have the member on their telephone call a specific line to verify, validate or confirm what their vote is, so anybody trying to alter a vote or manipulate things would have to have all that previous knowledge and be able to instantaneously change something in a way that requires calculation and time. They would also have to compromise the phone carrier and impersonate the member at the exact window of voting on that confirmation call.

All of this requires zero training on the part of the voting member. It is maximally and logically verifiable, and it is minimal on cost. The technology already exists to do it.

Thank you.

• (1255)

**The Chair:** Thank you, Mr. Vickery.

We're going to head into the question portion of the panel.

We'll begin with Mr. Brassard for six minutes, please.

**Mr. John Brassard:** Thank you, Madam Chair.

First of all, thank you to all the panellists today. You've given us very interesting information.

I want to get your opinion on the Zoom platform. Parliament has gone all in, as have a lot of other businesses, with this particular platform. As it relates to not just voting, but overall security of the platform, we're hearing today in a story from the Associated Press about censorship issues with China.

In the previous study we did, we were told that a lot of the data transmits through servers in Vancouver and Toronto, at least for business that's done in Canada, but there's seemingly no guarantee that that can happen. When the company was asked about what happened with respect to Hong Kong, it refused to comment on that.

Mr. Vickery, I'll start with you on the Zoom platform and your confidence. Obviously, a G7 country is a valuable target for state actors and non-state actors as well, so I'm just interested in your comments on the Zoom platform.

**Mr. Chris Vickery:** These comments are good for any similar commercial offering, not necessarily specific to Zoom but including Zoom. I would not do anything secret over Zoom or any other similar platform. You cannot be certain that there are not going to be adversaries listening or intercepting, or even changing packets and communications, because you don't know who is the third party contractor who may have access either overtly or covertly to something that widespread. It is just not trustworthy for anything of a high security nature.

• (1300)

**Mr. John Brassard:** Mr. Ghorbani, do you have comments in regard to that?

**Ali Ghorbani:** I will say similarly that Zoom is not unique in terms of security flaws. Any video conferencing platform would have issues. Zoom became famous with the Zoom bombing, etc., that happened recently, but they at least have openly reviewed a

proposal for end-to-end encryption that would be sufficient for at least the integrity of the data moving between the two ends.

In the end, I think your guess is as good as anyone else's. You could say Microsoft Teams has better security. At least they advertise it as having better security, and it appears to have good security in place, but all in all I think they are all going to be in the same group as being vulnerable to any third party type of attacks, networking, etc.

I did mention at the end of my seven-minute opening statement that the routing of the data is awfully important. Definitely Parliament should make sure how the data is routed and which part of the network the data actually ends up travelling through.

**Mr. John Brassard:** Thank you, Mr. Ghorbani.

Mr. Vickery, there are a couple of points I would like to make.

I'm very interested in the separate physical piece of hardware, the component you spoke about. I'm interested in how you see that potentially working.

I also want to bring you back to 2018. You talked about the idea of phone and Internet elections, and I will quote from when you were before the ethics committee:

Stay away from that. Use paper ballots with audit trails. As long as you're using paper ballots with audit trails, you're relatively on the right track.

Do you still stand by that view? Would your concern also extend to legislative voting in Parliament as well? There are two points there I would like you to address.

**Mr. Chris Vickery:** I absolutely still stand by that statement. The context was in a nationwide election with millions of people involved. If you're dealing with 200 to 300 elected officials, it is feasible to have them vote, and to confirm those votes, and to do so in a secure enough way that you can be confident in the result being accurate. It is much different when you're doing it with millions of private citizens.

**Mr. John Brassard:** On the issue of the separate physical piece of hardware that you referred to, what type of hardware would you be using? Would it involve an application? What's the potential cost?

I assume it's in development somewhere, but what would be the actual cost to implement that type of program? Can you expand further on that, please?

**Mr. Chris Vickery:** Well, this little thing right here is actually outdated. That's what I'm using as an example. It's a Packet Squirrel. It costs \$30 commercially to buy one of them. I'm sure you could get a whole bunch of them at a bulk rate. It is sold online. I have no financial ties to it. I don't stand to benefit from it whatsoever.

I'm saying basically it is a network tap type of device. You just plug it in and it is connected to the network. It has software that runs on it that is configurable by you. You can set it to communicate with only one specific IP address, and set it to communicate in a way that it does not receive commands and only sends them.

**Mr. John Brassard:** Okay.

The other issue you spoke about as well is the delay in a response to the actual vote. Can you provide a clearer—

**The Chair:** Unfortunately, that's all the time we have.

Do you want to get out the rest of your question? Maybe it could be responded to later.

**Mr. John Brassard:** How could the delay be measured? What examples would our security team or IT team on the parliamentary side be looking for more specifically when it came back to them?

Thank you, Madam Chair.

• (1305)

**The Chair:** Maybe one of your colleagues can pick that up as well.

Mr. Turnbull.

**Mr. Ryan Turnbull:** Thank you, Madam Chair.

Thanks to all the witnesses. I really appreciate the expertise you bring to this panel.

I want to start by mentioning the two doctors, Dr. Essex and Dr. Goodman, whom we had on this morning's panel. They made a very clear distinction between general election online voting and parliamentary online voting. They pointed to the fact that parliamentary online voting is a matter of public record. It relies on the federal government's cybersecurity infrastructure and the capacity our federal government has for training MPs.

Mr. Ghorbani, you mentioned in your opening remarks that people are the weakest link, and you stressed the importance of training MPs in any online or virtual proceedings so people are aware of the risks. Do you want to talk further about how we should do that moving forward, assuming we move forward with some form of online voting?

**Mr. Ali Ghorbani:** First, I think the issue of awareness has to be a continuous agenda within Parliament to make sure that every so often the members are aware and trained about the new issues and problems that come up. It's not one-time training and you're done with it.

Second, I would disagree to some extent that it really doesn't matter when it comes to general election online voting or parliamentary online voting. The two main issues in online voting are verifiability and availability, or you don't end up having a case where people cannot vote, or you want to verify their vote. It was mentioned also that maybe a phone call afterwards should be used to verify. The size is not important here; it's more that you want to make sure that a vote is done properly and is verifiable in the end.

Again, I want to emphasize your point. I'm a big proponent of the awareness issue of programs within different departments in the government, and Parliament would be no different.

**Mr. Ryan Turnbull:** Thank you.

Mr. Jourdan, you outlined quite an important list of points. I tried to write them all down, and I'm not sure if I got them all, but it sounded like you were very firmly in the camp that says this online voting is doable, based on what you know of much of the IT infrastructure, the cybersecurity infrastructure, that we have currently. Would you say that's true?

**Dr. Guy-Vincent Jourdan:** Yes, that's correct.

**Mr. Ryan Turnbull:** Would you be willing to table an outline with this committee of those specific points you made? I didn't quite get them all down. It seemed to resonate with the things we heard from our cybersecurity folks at the House of Commons. I value your points. Would you be willing to submit them?

**Dr. Guy-Vincent Jourdan:** Yes.

**Mr. Ryan Turnbull:** Thank you very much.

I want to talk about procedural safeguards. I know there are technological and procedural safeguards. We've heard about ensuring that members would verify their vote potentially in multiple ways, and that we have a plan. It certainly seems important to many cybersecurity experts to have a plan for what goes wrong, or when something goes wrong we know what to do.

Mr. Vickery, do you have any thoughts on that?

**Mr. Chris Vickery:** Yes. A way to mitigate the risk of a catastrophic event and single points of failure is to intertwine competing platforms within it. This means if you are sending a vote over the Internet, have it go to not only one cloud routing centre before it gets to the official site, but also send a mirrored, exact duplicate to the competing next company that is fighting with the first company for revenue. Have them receive it and perhaps hold it or even transmit it or let it be viewable to the receiving side, and if they don't match, you have problems. They should match.

Neither one of these companies wants to be known as the company that was compromised and votes were changed. They have a defined interest and a competitive interest in being correct, accurate and as ethical and well-regarded as possible, because otherwise the competitor is going to eat their lunch.

• (1310)

**Mr. Ryan Turnbull:** Mr. Ghorbani, do you have any thoughts on procedural or technological safeguards specific to online voting?

**Mr. Ali Ghorbani:** I would like to second what was said.

In order to make sure that we do have a secure, verifiable and available system, we need to work on diversity, basically. We could end up having two systems marrying each other so if one were closed down, the other one could actually hold on.

Diversity would be a core in terms of making sure that you have everything available at any time for voting to go on.

**Mr. Ryan Turnbull:** We've also heard the importance of simplicity in the design of the device for interface, programs, software, etc., that's being used for this in the future.

Mr. Jourdan, I wonder if you could comment on usability considering the amount of human error that can occur.

**Dr. Guy-Vincent Jourdan:** Yes, obviously, the—

**The Chair:** Unfortunately, Mr. Jourdan, that's all the time we have unless you have a quick yes-or-no type of response. I don't think for this question you might be able to.

**Dr. Guy-Vincent Jourdan:** No.

**Mr. Ryan Turnbull:** Thank you.

**The Chair:** Next up we have Madam Normandin.

[*Translation*]

**Ms. Christine Normandin:** I thank all the witnesses for their presentations, which I have found very enlightening.

I would like to put my first question to you, Professor Jourdan. You talked about existing voting systems used by private companies, including for shareholder votes. We have discussed the possibility, even the necessity, of having a portion of our vote be visual, or at least vocal. To your knowledge, does a system with a visual portion of the vote already exist on the market for other companies?

**Dr. Guy-Vincent Jourdan:** Yes. To my knowledge, some companies just use Zoom, where everyone takes their turn speaking and raises their hand. I think it all depends on the number of voters.

**Ms. Christine Normandin:** To your knowledge, are there any systems where a visual response can be recorded and passed on without necessarily going through Zoom, where people vote in succession?

**Dr. Guy-Vincent Jourdan:** I don't know whether such a system exists, but it can clearly be prepared and implemented.

**Ms. Christine Normandin:** Great, thank you very much.

Moreover, complementary to the list request my colleague Mr. Turnbull sent to you, I note that there is already a list of criteria at the U.S. National Security Agency that helps determine whether one system is more suitable than another. If that list is different from the one Mr. Turnbull asked you for, I would like you to please send it to the committee if possible.

**Dr. Guy-Vincent Jourdan:** Okay. I will send you the document, which is in English.

**Ms. Christine Normandin:** That's fantastic. Thank you very much.

You brought up the importance of having a registry of the issues arising during the use of a system and of having an emergency plan. You also talked about the resources currently available at the

House of Commons. To your knowledge, are those resources sufficient to implement this kind of a plan and to keep such a registry?

**Dr. Guy-Vincent Jourdan:** It is difficult for me to answer. I know that you have a very good base.

As far as I understand, the infrastructure is in place. I think the ability to keep registries also already exists, as there is really nothing exceptional to that.

Do you need to hire more people? I cannot speak to that, but I would not be surprised if you did. However, I don't think that you need to make massive hirings, as you already have a solid team.

**Ms. Christine Normandin:** Thank you.

I now go to you, Mr. Vickery.

We discussed the visual portion of a vote, a notion that seems to greatly interest members. I would like to know whether the unidirectional communication system you have presented to us would also enable us to send a recording of a visual vote and whether it would protect us from a risk of deep fakes?

• (1315)

[*English*]

**Mr. Chris Vickery:** The answer is, yes, it could be used to send.... However, I would advise against relying on a visual or video-type of vote. You are going to have problems as technology advances with abilities to forge and manipulate those types of things. It is a losing battle and it is not future-proof.

[*Translation*]

**Ms. Christine Normandin:** However, can it be combined? Can we have several vote validation methods, including a visual vote?

[*English*]

**Mr. Chris Vickery:** Yes, that is actually a very good idea, and it could be used as a layer on top. That would also deter bad actors, because if something shows up anomalously, you're going to know where to start investigating.

[*Translation*]

**Ms. Christine Normandin:** I have another question for you, Professor Ghorbani.

You talked about the human factor being the main concern. Can you specify in what way the human factor can be especially critical for an electronic vote?

[English]

**Mr. Ali Ghorbani:** Fundamentally, this probably would be the case where the person does not use the proper equipment or system and software, so a third party could get in between, and the data in transit could be altered or changed, etc. That's how I can see it from the human perspective: an error to allow a vote to be altered and changed. It also makes a good understanding from the perspective of a person to be educated about encryption and how, from her end, data can be encrypted and sent to the other end so that the data in transit will not be altered, changed or grabbed. That's how I see it from the human perspective: errors that could be made.

[Translation]

**Ms. Christine Normandin:** Thank you very much, Professor Ghorbani.

Madam Chair, it appears that my time is up.

[English]

**The Chair:** Next up is Ms. Blaney, please.

**Ms. Rachel Blaney:** I want to thank all the panellists for being here with us today as we discuss this very important matter.

I would like to bring the first question to Mr. Jourdan. We are hearing from some of our witnesses today and heard in our last report that the security of virtual Parliament operations is not purely technological. There are human considerations that need to be accounted for.

Do you think members and staff should be involved in the development of a remote voting solution? What kinds of training and protocols need to be in place for the human element of remote electronic voting to be done safely and securely?

**Dr. Guy-Vincent Jourdan:** Yes, absolutely. I come to this debate as a technologist, so I have a technological point of view, but there is absolutely no question that a good system is going to involve non-technical people and users in the first place. So yes, I absolutely agree that this is not something that should be done just by IT folks.

I was just saying that in terms of training, of course, it would be fundamental to have regular training and updates. Such a system is going to be.... We uncover problems all the time, so a system like that would have to be agile. They would have to give upgrades regularly, and that means that people would have to be retrained constantly. That has to be taken into account. That has to be part of the plan.

**Ms. Rachel Blaney:** I couldn't agree more.

Mr. Ghorbani, do you have anything to add to that?

**Mr. Ali Ghorbani:** Sure. I think what is important to recognize here is that when we talk about training, it is not that IT people are always being trained or that they have to be front of people to train them. We need to bring people with all sorts of expertise into the conversation, such as groups from business, law, education and the humanities, including sociology and psychology. They are all important elements when we talk about an awareness programs in cyberspace. If there is a training program and it's going to be an ongoing kind of program, you want to involve these kinds of expertise

as part of developing the contents and delivering the finished project.

• (1320)

**Ms. Rachel Blaney:** One of the concerns I've had through this process is that we have a very large country, and connectivity in some of our ridings is a concern. I think addressing that issue is really important. Part of having all MPs participate, especially those of us who are in more remote ridings, is that it simply makes sense. We'll be able to identify any gaps.

I'm wondering if you have any suggestions on who we need to include and whether all MPs should be included in the process.

**Mr. Ali Ghorbani:** To my mind, if you're asking me, all MPs should be included in this process.

A couple of years ago, we were in front of a few MPs to show them how easily they could be attacked or hacked through their phones or their laptops. It's important that all MPs get the training, and also continuously get the training. As we know, we are continuously getting new types of attacks. There are new types of phishing and new ways of manipulating and spoofing and so on.

It's important to have everyone involved.

**Ms. Rachel Blaney:** Thank you.

Mr. Ghorbani, and then Mr. Jourdan, comparing the digital security of different methods of recorded or roll call votes, how would you compare video voting through a video conference platform with remote electronic voting on a House of Commons-managed device? Are they both safe?

**Mr. Ali Ghorbani:** To me, they are as safe as they can be right now. They are safe, but as I said, the only thing I'm concerned about is the verifiability issue. There has to be a plan in place by the House in order to verify the total tally, the details of the tally, and also the availability issue. As you mentioned, for many people who are in different ridings and who may not have good connectivity, a small-scale denial-of-service attack could actually easily prevent people from voting.

Both technologies do suffer from both items that I mentioned: verifiability and availability.

**Ms. Rachel Blaney:** Mr. Jourdan, do you have anything to add to that?

**Dr. Guy-Vincent Jourdan:** Yes. I would like to go back to your point about bandwidth. I think there is one difference between those two approaches. That is, in the system we're talking about with a dedicated messaging system, a dedicated voting system and a dedicated video conference system, the one that is hungry for bandwidth is the video system. So I would be a bit worried about putting the vote part onto that. It's the one that's most likely to break if you have poor bandwidth.

I would also echo my colleague's comments regarding the availability. In terms of security, if I had to identify what would be of topmost concern to me, because of the context of these votes, I think availability would be of most concern. It would be quite difficult to change someone's vote so that no one saw that, but it would probably be easier to prevent the voting in the first place.

That probably would be a good place to focus the attention.

**The Chair:** Thank you so much, Dr. Jourdan.

Next, from the Conservatives, we have Garnett....

How do you pronounce your last name? I still hear it pronounced a couple of different ways.

**Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC):** It's "Jen-us", typically. It's an unfortunate anglicization from the original Maltese. You know, "Jen-o-eez" is the original Maltese. I hope this doesn't cut into my time, but I could explain the origin of my last name.

**The Chair:** Next time.

**Mr. Garnett Genuis:** Next time we have one of the longer sessions that we have from time to time in PROC, I will go into more detail on that.

**The Chair:** Absolutely.

Mr. Genuis, you have five minutes, please.

• (1325)

**Mr. Garnett Genuis:** Okay. I'll be briefer than usual.

Mr. Vickery, it was interesting to hear your discussion of a method that would work for voting that would be secure. Of course, here we're concerned about two possible kinds of vulnerability. One is the issue of foreign interference, of hacking. You explained how that risk is mitigated with the method that you've proposed.

There is another kind of risk, however, and that's MPs effectively giving up what is supposed to be their responsibility for voting. They might hand over the device you've discussed to a member of their staff or a member of the whip's staff. They might say, "I'm going on vacation for the next couple of days. Just vote the party line." This sort of thing theoretically would involve the active cooperation of the member, but would still be something that would be very inappropriate. We'd want to make sure there was a system to prevent that from happening, because it's the responsibility of members to vote, to be seen to vote, and to vote themselves, whatever influences are taken into consideration.

Does your proposed method of a prescribed piece of technology do anything to address that possible risk of someone giving the device to somebody else to vote for them, forwarding email codes and those kinds of things?

**Mr. Chris Vickery:** Absolutely. In order to have that happen, the proxy person, or whoever, would have to physically be in the residence in order to have the IP address that it is sent from and known ahead of time to be received from. That validates, at least from a physical perspective, that where that IP address is located is at their home. Then you would have them confirm via a phone call, using their own voice, within a specific window of time. You know their

phone number. Their number can't theoretically be spoofed. That's illegal, I would assume, in Canada as it is in the U.S. So, you not only have voice, phone number and specific IP address, you can add in other identifiers that are specific and unique.

**Mr. Garnett Genuis:** Just so I understand, then, you're saying that basically the only way to go forward with this is to have those multiple levels of redundancy. You have the direct piece of technology. That has to be tied to a location as well as some kind of voice verification. All of those levels of checking would be necessary to achieve the result that you're talking about.

**Mr. Chris Vickery:** I would summarize it as a second band of confirmation, some sort of non-connected secondary confirmation method that is out of the original network.

**Mr. Garnett Genuis:** It's interesting because we're already doing some of this. We have supposedly in-camera meetings of PROC that have happened on the Zoom platform with nothing resembling that level of background here. It seems that, based on your testimony, the systems that we have in place are so far behind in terms of essentially assuming that we can just use Zoom and call it in camera and everything would be fine.

**Mr. Chris Vickery:** It may work. But over time, it will head south as far as integrity and belief in the system go. It will only degrade.

**Mr. Garnett Genuis:** Some people out there might be wondering: Is this actually really a concern that people want to interfere with these kinds of meetings? It's worth members looking at the 2019 report of the intelligence committee of parliamentarians, which shows that there are major, growing issues of foreign-state interference and that Canada is, frankly, way behind on being aware of and responding to and coordinating these issues.

Could you maybe just underline whether it a realistic concern that there are actors, foreign states, trying to interfere in our democracy that would have an interest in identifying these security vulnerabilities and exploiting them?

**Mr. Chris Vickery:** Absolutely. I steadfastly believe there is an undeclared world war, practically occurring as we speak, against democracy and everything that it stands for. So yes, there are lots of people, both for profit and for political ideology purposes, around the world actively, 24 hours a day, trying to cause harm to Canada, as well as to others.

**Mr. Garnett Genuis:** You talked about how those vulnerabilities exist on multiple different platforms. Is it a particular concern that we're using right now a platform that is under the potential influence of the Chinese government, with what we've seen in terms of back doors for technology with Huawei? There was a situation where the Chinese government built a building for the African Union that was found to be full of listening devices. There are so many different cases of influence. Is this a particular concern for you that you think we should be sensitive to?

• (1330)

**The Chair:** We're over time.

Next up, we have Madam Petitpas Taylor.



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

I also would like to take an opportunity to thank our witnesses who are with us today, with a special greeting and shout-out to Dr. Ghorbani, who is a fellow New Brunswicker as well.

First of all, this morning we heard from an esteemed panel group as well, and the representatives spoke to us about the importance of developing a cyber-incident response plan in the event that we had a threat that had been identified in an attempt to disrupt or compromise our systems. I am not an IT expert at all. I'm wondering whether all three of you could provide us with the elements that should be included in a cyber-incident response plan to ensure that we can better understand what that would entail.

Maybe I'll start with Dr. Ghorbani.

**Mr. Ali Ghorbani:** Thank you very much, and hello to you from New Brunswick.

Yes, the cyber-incident response plan is an integral part of any plan you must have in your organization when it comes to cyberspace and cybersecurity, that's for sure, but we also have to recognize that we have a fairly advanced group of people and infrastructure within the Communications Security Establishment that provide these kinds of services, and they're also in charge of Cyber-Secure Canada. So, yes, a collaboration between Parliament and CSE would make sure Parliament does have a cyber-incident response plan in place for things that might happen as a result of a breach in cyberspace.

**Hon. Ginette Petitpas Taylor:** Thank you.

Monsieur Jourdan.

**Dr. Guy-Vincent Jourdan:** Yes, I will second what Mr. Ghorbani just said. We obviously need that. In Canada we have the kind of knowledge to gather this kind of plan and have it in place to end all that.

I would simply state the obvious, which is that it's not related to what we are talking about right now. It has to be in place right now, because you are already using technology to do all kinds of things. I think we want to look at the proposal on the table today in the context of what we have. We are not changing or introducing something crazy here, compared to what is already happening. I expect that plan to be in place right now, and I think we should maintain it and have it address this new situation.

[*Translation*]

**Hon. Ginette Petitpas Taylor:** Thank you, Mr. Jourdan.

[*English*]

Mr. Vickery.

**Mr. Chris Vickery:** The plan I would have in place, and if you do not, you need to get it in place, is one to immediately mitigate the compromise. Don't necessarily turn everything off, because you can lose valuable forensics that way, but segment and mitigate it. Have defined roles ahead of time so people know their job in an incident response situation, and they're not left guessing or checking with somebody else to see if they need to do this, that or the other.

If critical infrastructure is involved, communicate with federal-level authorities early on, very quickly, to see if you need to do anything to help their investigation. If they are investigating an advanced, persistent state actor, and you were to turn off systems immediately and lose some valuable forensics, it would be a tragedy.

I would do those things.

• (1335)

**Hon. Ginette Petitpas Taylor:** Thank you.

I have a very quick question. I know I only have about 30 seconds, so perhaps I'll get a yes or no answer from all three panellists.

We're not looking at creating anything very complicated. We're looking at moving forward with a voting system with respect to legislative votes that have already been done in public, that are being done publicly, and also looking at a hybrid system when we're debating in Parliament. Again, everything is public, nothing is confidential. Do you feel we have the technology available to do that securely?

Mr. Ghorbani.

**Mr. Ali Ghorbani:** Verify it in the end, but, yes, we do.

**Hon. Ginette Petitpas Taylor:** Mr. Vickery.

**Mr. Chris Vickery:** Absolutely. It just has to be done correctly.

**Hon. Ginette Petitpas Taylor:** Mr. Jourdan.

**Dr. Guy-Vincent Jourdan:** Yes, and it's inherent that it has to be done correctly.

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

Mr. Richards, please go ahead for five minutes.

**Mr. Blake Richards:** Thank you.

Mr. Vickery, Mr. Genuis asked you a question and, unfortunately, time ran out. I'd like to give you an opportunity to respond to that question. Do you need me to restate it?

**Mr. Chris Vickery:** Could you summarize it?

**Mr. Blake Richards:** Sure, I can do my best, and, Mr. Genuis, feel free to pipe up if you think I've mischaracterized it.

Essentially, what he was asking you about was the fact that we are using a platform right now where obviously there is a significant amount of control by state-owned Chinese involvement.

**Mr. Chris Vickery:** I recall that.

**Mr. Blake Richards:** I'm wondering if you had any thoughts on whether that's something we should be cautious about and whether you would have concerns about that.

**Mr. Chris Vickery:** I would not be talking about anything secret on this type of communication, because it's a public, open knowledge type of forum. It's probably okay, but I would not translate anything that needs to be kept confidential over this platform or any other commercial generic offering out there.

The Chinese side of things is a state-level concern, so it is elevated. I wouldn't say that they are the highest level of concern out there, but it is an elevated concern.

**Mr. Blake Richards:** Thank you. I appreciate that.

Given some of the testimony that we've heard here, some of the responses we've heard today—Mr. Brassard, I think, pointed to a report that we're seeing about some rather interesting things that have happened with Zoom—and the fact that some of the members of this committee have tried to get answers to this from the administration previously as well as from Zoom, I want to move a motion.

I'll read it slowly because then translation can keep up, so that it is in both languages.

I move:

That the committee order the House of Commons Administration to produce, no later than Monday, June 15, 2020, all contracts, master service agreements, licensing agreements and terms and conditions, including and in respect of data collection, use and disclosure of personal information and third party contractual arrangements that it has entered into with Zoom Video Communications, Inc. and any of its subsidiaries, affiliates or agents.

**The Chair:** All right.

You still have time on your questioning.

**Mr. Blake Richards:** I'm recognizing the fact that we don't have a lot of time with these witnesses and I don't want to use a lot of the time. I would like to see a vote on this motion, so perhaps we could proceed if there is any debate or proceed with the motion, because I would like to make sure that we don't steal any more time from witnesses.

**The Chair:** Okay.

Justin, could you just speak to the committee as to how we can proceed?

**The Clerk of the Committee (Mr. Justin Vaive):** Mr. Richards just moved a motion. Generally at this point the committee would open the floor for debate until such time as debate is over, and then the committee would make a decision on the motion Mr. Richards just moved. The committee can also decide to continue with the questioning and then come back to Mr. Richards' motion afterward, if that is acceptable to the committee. It's really in the hands of the committee. It would take the consent of the committee to agree to do that.

Otherwise, the normal course of things would be that once a motion is moved and proposed, debate would follow, followed by a decision once debate is finished.

• (1340)

**The Chair:** Mr. Gerretsen.

**Mr. Mark Gerretsen:** Thank you, Madam Chair.

I'm very happy to discuss this motion. I wouldn't mind if we could just move to defer it until after we're done with the witnesses. I think we only have two or three more questions. Then we can let the witnesses go and do this.

Is Mr. Richards okay with that?

**Mr. Blake Richards:** I'd like to see us proceed, just to make sure that we deal with the motion.

I was hoping that maybe it could be voted on quickly. I would think that it's something we could all agree to.

**Mr. Mark Gerretsen:** Yes, I'm happy to vote on it.

To be completely honest, Madam Chair, I don't even have a problem with the motion. I just wanted to give the opportunity for people to debate it without holding up the witnesses who are here. I just thought I'd throw that out there.

**The Chair:** We do have committee business time, but if the committee wishes to vote on it right now, if there isn't much debate, then I don't see why that would be an issue since we won't be holding up the witnesses if we can get to a quick vote. However, if there's a lengthy debate, maybe we can save it for committee business time.

**Mr. Mark Gerretsen:** June 15 would be Monday of this coming week. Was that the date you said, Mr. Richards?

**Mr. Blake Richards:** That's the date I gave.

**Mr. Mark Gerretsen:** My only concern would be that we're really only giving one business day to produce this. If they can do it, that's great. I imagine that if there is a timeline problem there they'll let us know, but I am happy to support the motion, Madam Chair. I think the more information we can get, the better.

**The Chair:** Mr. Turnbull will speak, and then Mr. Alghabra.

**Mr. Ryan Turnbull:** Thank you, Madam Chair.

I didn't really catch all of Mr. Richards' motion. I know he read it fairly slowly, but maybe my mind was elsewhere at the moment. I really didn't catch the full scope of the motion that Mr. Richards put forward. I wonder if we could either request it in writing or have it read out really slowly again. I'd like to write it down if possible.

**The Chair:** Okay.

Before we go to that maybe we can hear from Mr. Alghabra, and then we can have Mr. Richards reread the motion.

**Hon. Omar Alghabra (Mississauga Centre, Lib.):** Thank you, Madam Chair.

Mr. Richards, I understand the idea behind it and the principle, and I'm supportive of it. Can you explain the relationship between the value of the contract and the study we're trying to do, for my own understanding and to see what the purpose is behind this tight timeline?

**Mr. Blake Richards:** Well, first of all it's not just about the value of the contract. It's about the terms and conditions of the contract, so obviously those could be material to what we're discussing.

As for the timeline, at present we're asked to report back by June 23, and we need to have the information. I don't see what the rush is, but there seem to be some members who feel there is one; therefore, this needs to be a rush too.

It still gives them two and a half business days to complete the request, and they should have this information on hand and easily available.

**The Chair:** Mr. Gerretsen will speak, and then Mr. Turnbull.

**Mr. Mark Gerretsen:** I was just going to add, Madam Chair, that there is the issue that, I imagine, the contract is written in English. There is going to be the issue of having that completely translated.

I think we vote in favour of it and if they are unable to produce it, then they'll give us a reason why it's going to take a couple of extra days to do that. I'm content with the date, providing that those who are responsible can come to the terms in time.

**The Chair:** Mr. Turnbull will speak, and then Mr. Alghabra.

**Mr. Ryan Turnbull:** Along the same lines as my colleague, Mr. Gerretsen, I was going to say that I think it's going to take some time to translate. I wonder if we could set a different date from June 15, which seems a little bit tight in terms of a time frame. Maybe we could give another three days or two days, or something reasonable like that.

Mr. Richards, would you be open to that?

**Mr. Blake Richards:** No, I'm not open to that. This should be easily available. It should be able to be done by that date.

As Mr. Gerretsen has indicated, if they feel for some reason they can't do that and they want to come back to the committee and indicate that there is a problem with that, then we can figure how to deal with it.

Frankly, you have to ask for something and you have to put a deadline on something. If they feel they can't comply, they'll have to explain why that is. I don't think we should be letting someone off the hook that easily.

• (1345)

**The Chair:** Mr. Alghabra.

**Hon. Omar Alghabra:** We are also discussing whether we are going to give ourselves a week or so to write the report, so that there is a little bit more time. However, Mr. Richards seems, for one reason or another, determined about the date. I don't know if I'm going to die on this hill, so I have no problem with it. I was looking for a way for all of us to compromise on moving forward, but I'm not going to fight hard.

If the House of Commons says it can't meet the deadline, it can write to us and explain why.

**The Chair:** Ms. Blaney.

**Ms. Rachel Blaney:** I just want you to know that I am ready to have a vote at any moment here. I think I would like to get on to the witnesses as quickly as possible.

**The Chair:** Mr. Reid.

**Mr. Scott Reid:** Just to say that in the event that the contract is long, I don't think we need to translate all of it. We just need to translate the pertinent parts, and perhaps we can rely on our clerk to make that decision for us.

**The Chair:** Perhaps that's doable. That's a good point you have raised, Mr. Reid.

Let's move forward with the vote.

We'll have a recorded vote on this.

**Mr. Ryan Turnbull:** Madam Chair, can we still have it read again? Thanks.

**Mr. Blake Richards:** I move:

That the committee order the House of Commons Administration to produce, no later than Monday, June 15, 2020, all contracts, master service agreements, licensing agreements and terms and conditions, including and in respect of data collection, use and disclosure of personal information and third party contractual arrangements that it has entered into with Zoom Video Communications, Inc. and any of its subsidiaries, affiliates or agents.

**The Chair:** Has everyone been able to follow the language of the motion? I see nodding.

We'll proceed to a vote.

**Mr. Mark Gerretsen:** Madam Chair, can we use Mr. Vickery's device to vote on this?

**The Chair:** Maybe at a future time, Mr. Gerretsen.

(Motion agreed to: yeas 11; nays 0)

**The Chair:** Thank you.

Sorry, Ms. Petitpas Taylor, I didn't see your hand go up. Would you still like to comment?

**Hon. Ginette Petitpas Taylor:** My only comment, Madam Chair, is that I want to ensure that all documents are translated. It's unfair to say that just parts of the documents are going to be. We need to have full translation of those documents.

**The Chair:** Thank you for that.

We will proceed, although we have lost quite a bit of time.

Mr. Gerretsen, for five minutes of questions.

**Mr. Mark Gerretsen:** Thank you very much, Madam Chair.

I want to go back to Mr. Jourdan. To be clear on what you said earlier, you think a voting system that is web-based or application-based, something along those lines, would be more inclusive of all members, in particular those who might be struggling with Internet bandwidth issues. Is that correct?

• (1350)

**Dr. Guy-Vincent Jourdan:** As I said, the system that is going to be the most hungry for bandwidth is a video system, so anything that is not video-based would be better.

**Mr. Mark Gerretsen:** Okay.

Mr. Vickery, you told us earlier not to rely on video. This is interesting because in the previous panel we had, most if not all the witnesses emphasized that their preference was video. At least one or two of them did make the point that this was notwithstanding deepfakes and the possibility of this stuff down the road, but they all seemed to put emphasis on video voting, as opposed to a web-based or application-based system.

You are taking a different approach. You're basically saying that we should be concerned about deepfakes because the possibilities of them only become more real as we go down the road, and that, therefore, we need something more secure. Is that correct?

**Mr. Chris Vickery:** That is correct. However, keep in mind the aspect of a necessary second or third band of confirmation, which is not involved with the video system. This could be added as a way to validate it or make it good enough. You have to have that other validation.

**Mr. Mark Gerretsen:** Let's keep in mind that absolutely every vote that we take in Parliament is open and public, with the exception of one or two circumstances like electing a Speaker and one issue that relates to private members' business that doesn't come up that often. Everything else is a public vote, so we're not worried about keeping that vote secret.

Does that impact your position? We'll always be able to know. It's not as though I vote and my vote can be changed and I'll never know about it. If there's a leaderboard or something displayed somewhere online, I can always look at that and say, "Hey, hold on. I voted no, but it says yes." The fact that we're open and everything is public makes the accountability of it fairly reliable. Is that correct?

**Mr. Chris Vickery:** It does tend to help; however, the degradation in people's belief in the system being accurate, the very existence of the possibility that somebody could, even temporarily, be recorded in the wrong way tends to harm that system overall—

**Mr. Mark Gerretsen:** Absolutely.

**Mr. Chris Vickery:** —and people's understanding that there are multiple layers of confirmation that always exist is a good thing.

**Mr. Mark Gerretsen:** You made a comment in response to Mr. Genuis's questions advising us not to talk about anything private in these meetings. Again, anything we say in the House of Commons is public. The delay between our conversation now and what's streamed online for the public to see is less than 10 seconds, so everything is out there; everything is public.

When you talk about the security issues and your concerns about them, do you have some comfort in knowing that everything is public in using this platform like that? The worst thing that can happen is somebody getting in and trying to take over the meeting or something like that, but it's not as though there are going to be state secrets that are shared as a result of somebody hacking in.

**Mr. Chris Vickery:** I would say the worst thing that could happen is that somebody's individual device is compromised and the audio is being manipulated to make it sound like they said "no" when they meant to say or did say "yes".

**Mr. Mark Gerretsen:** You don't even need the device compromised. A witness in the previous panel told us as an example that, in a city council meeting in Sarnia, somebody said "disagree", and the person recording it heard "agree" but didn't hear the "dis" part. That created confusion.

• (1355)

**Mr. Chris Vickery:** That is absolutely a concern, and that's why multiple layers of validation are important.

**Mr. Mark Gerretsen:** Thank you.

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

Madame Normandin.

[*Translation*]

**Ms. Christine Normandin:** I have only one question for the three witnesses for my own knowledge. Aside from using an IP address to identify voters, we have talked about using biometric data. I would like to know what that implies.

Does the House already have that data? Is there a risk of that data being stolen and, therefore, a risk of identify theft. I would like to hear your general thoughts on that.

**Dr. Guy-Vincent Jourdan:** I will begin.

I think this is an important issue to raise. The voter can be identified in ways other than through the video. If we just want to make sure that the correct person voted, a biometric identification through the device can be done at the time of the vote. Presumably, you all have in your pocket a telephone that knows how to do that. It knows how to recognize your face, your fingerprint or something like that. That can be done locally, and it is related to your identity.

Your actual identity is not sent to the server. For example, we can easily imagine a very simple application that, at the time of the vote, would ask you to select yes or no and to confirm your identity by putting your finger on the telephone or by looking at it. That makes it possible to link your identity to your vote without having to send a video in real time.

[*English*]

**The Chair:** Mr. Ghorbani, do you have a response to that?

**Mr. Ali Ghorbani:** I really don't. It's important to recognize that authentication to multiple layers, including biometrics, would add more security to the operation. As mentioned by Guy-Vincent, it's easy to implement it. In short, yes, this might be a good thing to consider, using biometrics to authenticate people.

**The Chair:** Thank you.

That's all the time we have.

Ms. Blaney, please.

**Ms. Rachel Blaney:** I have just one question, and I would enjoy hearing from all of the witnesses.

One of the realities I've heard from multiple MPs is about living in family circumstances during this time and looking at other issues like being able to have that connectivity. These are some things they're concerned about. They want to make sure that voting is predictable and that there's a specific time, perhaps once a week, when all the votes happen so they know when they have to be there and they can make sure they're somewhere where they can physically vote with that connectivity.

I'm looking at it from that perspective of certainty. Are there any particular security concerns that we should consider if we're looking at having a time when we regularly vote?

Mr. Jourdan, we could start with you.

**Dr. Guy-Vincent Jourdan:** Off the top of my head, I don't see any particular security issue linked to the time of voting. I think that's what you mentioned here about family being around. Some obvious points would be not to share the device with the family and to make sure that you use only dedicated hardware and a secure link if you can. However, I don't see any obvious reason why we should worry about a particular time of voting.

Again, I would stress the fact that.... I think if the Chinese want to do something to us, they are not going to do that, try to change your vote from yes to no from time to time, because you will see that right away. No, I would not be too concerned about that.

**Ms. Rachel Blaney:** Thank you.

Mr. Ghorbani.

**Mr. Ali Ghorbani:** I do not have much of a concern except that, of course, we are giving the malicious people a schedule, so they actually know and can be prepared. To some extent, if it is public and it is getting into the hands of everyone, those who are malicious are better prepared at the scheduled or planned time when the voting would happen. Other than that, it's not going to be a big deal.

• (1400)

**Ms. Rachel Blaney:** Thank you.

Mr. Vickery.

**Mr. Chris Vickery:** I think that can be improved upon and is workable. If you have, for example, a period of one hour on a Tuesday every week when you take these votes, you can assign windows of time, so that during these five minutes of that hour, X, Y and Z members can send their votes in. That's not publicly broadcast; that's just decided in the moment. Then the bad guys will know the window overall, but they will not be able to predict these specific windows of a few minutes when it is valid for certain members to send their votes in.

**The Chair:** Thank you. That's all the time we have for this panel.

I want to thank all the witnesses. Mr. Ghorbani, Mr. Jourdan and Mr. Vickery, you've all been excellent, and not just for this study. From time to time, some of you have helped the House of Commons and have advised us on how we can maintain a secure and safe democratic system. Thank you for that.

Now, if I can ask the witnesses to leave the meeting at this time, we can carry on with some committee business.

[*Translation*]

**Dr. Guy-Vincent Jourdan:** Thank you.

[*English*]

**The Chair:** All right. We're right at two o'clock, so I'm hoping we can move along really quickly.

I guess my first question to the committee is this. Last time I was sensing.... Well, I wasn't just sensing it. Quite literally, a lot of comments were made by people wanting to have an extension and not feeling that there was enough time in two meetings next week to work on the draft report and review it properly, and also, if there are any supplementary or dissenting opinions, not enough time for that. I know there were also comments saying that there was understanding for that.

I just wanted to know where the committee was at, and whether the whole committee.... Essentially, if that's where we're at and if that is what we're asking for, if we want an extension, I would like to table a report back, hopefully tomorrow, asking for a specific extension date because we would not be able.... Essentially, we need approval for an extension, so the House would have to concur, but because we don't have routine proceedings, the House will not be able to concur. Especially if we leave it until the 23rd, that will not be possible, but there is a procedure in place whereby the four House leaders can agree to give this committee the extension we require.

I want to be able to give them the appropriate time to give that to us so that we know what we're dealing with next week. Is there a date? Is there agreement, first of all, on having an extension past next week? If so, is there a date that you would like to see?

I believe there are some hands up from the previous dialogue. Could you take your hands down and then raise them back up for this?

Mr. Gerretsen.

**Mr. Mark Gerretsen:** Mr. Reid's hand is still up from last time.

**Mr. Scott Reid:** I forgot to take my hand down, so just ignore it.

**The Chair:** Thank you. You can raise your hand again if you'd like to participate in this portion of the discussion.

Mr. Gerretsen.

**Mr. Mark Gerretsen:** Thank you, Madam Chair.

I respect the discussion and respect the comments that have been made, in particular by the opposition, about the need for rushing. I am certainly in the camp that wants to make sure we have a thorough report. I don't want to have the same scenario where we had an extremely long meeting last time, despite the fact that I was driving home from Ottawa during a lot of it.

I respect that, but I don't want to let this drag on and on. If we're going to be asking the House to do something—and presumably that would be for September—then we need to make sure that we give enough time to whoever has to do it. Therefore, I would propose that we ask for an extension until Friday, July 10, which would give us two and a half weeks more than what we currently have. I'm open to hearing what other people might have to say about that.

● (1405)

**The Chair:** Okay. We discussed last time how from June 23 or 24 to July 3 we would not be able to have any meetings, either virtually or in any way, because there's testing happening. That would leave us a week at that point, but you would have all the other time that we are not able to meet in order to write and reflect.

We would have one week of meeting time, and we could have some meetings in there, too, if you feel that meetings are necessary. It all really depends, I think, on how far we get next week, to see how many meetings we would need in that coming week. Or we could propose another date.

**Mr. Mark Gerretsen:** My thought, Madam Chair, was that it would be up to June 23, when we would conclude with any other witnesses or any other discussion we want to have about it, so that we can then have our time to go and craft our recommendations over that down time you mentioned.

**The Chair:** Okay.

Is there any opposition to asking for an extension until July 10? There were quite a few people who had comments about not having enough time and feeling that they were rushed, so would everyone be...?

**Mr. Turnbull,** I think you're putting your hand up right now. Is there something you'd like to say?

**Mr. Ryan Turnbull:** I just wanted to say I'm fully in support of that date.

I thought maybe I'd clarify. Last time, we had some discussion about witnesses, and I really felt like this Friday.... I think we have a meeting tomorrow for one hour with an additional witness. Is that right? I was wondering if that could be the end of the witnesses, given the fact that I think what I heard is that we're likely going to need four meetings.

Based on how long it took to write a report last time, and to avoid that eight-hour push at the end, maybe we'd have.... As you said, we can't meet from June 23 to July 3, so extending it to July 10 effectively gives us the ability to have two more meetings in addition to the two meetings next week, if I'm not mistaken. Is that right?

**The Chair:** Yes, we can squeeze in the two. Depending on how many committees want to go, we could probably have more meetings than just the two that week, but I can't guarantee that, as it's not our dedicated time slot.

The House administration team has been quite accommodating in the past, so we could even do three, I would think.

**Mr. Ryan Turnbull:** My only point was just to clarify that we probably need three, maybe four meetings to get through the rec-

ommendations and get some agreement on how to move forward. That was my thinking.

**The Chair:** Yes. We would definitely have two next week. We could schedule two in that week. I'm just saying that if the committee feels it needs even more than the two meetings a week, I can at least request it. I just don't know whether there will be a time slot available, but sometimes they are able to accommodate.

**The Clerk:** Madam Chair, I just want to point out to the committee that a deadline of July 10 would actually enable the committee, if that were the will of the committee in terms of the consideration of a draft report, to have meetings on June 16, 18, 23 and 25, and then in the additional week, on July 7 and 9. Some of those dates, especially in the run-up to July 10, would obviously be needed for production purposes and translation purposes, to finalize the report and have it fully ready to be sent to the office of the Clerk of the House.

There may be some difficulty with meetings in the week of July 7 and 9, depending on outstanding production work that would be needed to finish off the report.

**The Chair:** Maybe the analyst, Andre, can help us with this as well.

I know you've already sent a portion of the draft report to translation, and I have just heard—this is for the benefit of the whole committee—that by Monday we might be able to get in our hands a portion of the draft report—a large portion, I heard—so we'll have something by this Monday.

Andre, what kind of time do you foresee will be needed when looking for an extension? Do you think we need to extend into one week of July, two weeks of July or more than that?

● (1410)

**Mr. Andre Barnes (Committee Researcher):** Thank you, Madam Chair.

To use a phrase that's been used maybe too much today, it is really the will of the committee as to how long the extension would be and how many more meetings you'd like to have.

A portion of the draft report has gone to translation. It might actually be translated by now. I'm writing a portion of Tuesday's meeting as we speak, and when I leave this meeting, I'm going to try to complete another portion, which will all be ready for Monday. Today's meeting will not be ready for the Tuesday meeting, just because it is practically impossible.

That is the update from my end. I hope that's enough to go on.

**The Chair:** When would today's meeting be ready?

**Mr. Andre Barnes:** It would be ready for Thursday, hopefully. Sorry, let me get that exactly correct. That would be the 18th.

**The Chair:** Okay.

Is there any other feedback?

If we are looking for an extension, I need to report back. That's the urgency of this matter. I can't wait until the 23rd to make this decision. I think our clerk can explain that a little better.

Mr. Richards.

**Mr. Blake Richards:** I think there were two different schools of thought on the rushed nature of this. This potentially satisfies one of those schools of thought. I might suggest a bit of a change, and maybe it's just a flexibility thing or whatever it might be. I like the way our clerk has laid out what the effects of this would be.

The idea is that we would get the rest of June essentially to finish with witnesses or whatever else we need to hear. Then, perhaps, rather than prescribing an exact date, we could simply say that following the blackout—I forget the period of time that we're blacked out for—based on the advice of our clerk and our analyst based on where they are at with things, we would pick up to write it in either a report or an interim report, whatever the case might be.

I would assume that's only going to take a couple of meetings, but if it takes three or four meetings or whatever, then so be it. I don't think there's a huge panic over July 10 rather than July 15 or something, or that some major catastrophic occurrence would happen if it was an extra few days.

Maybe rather than extending to a specific date, we could simply say that we will continue to hear from witnesses until June 25 or whatever it was, and then, following the blackout period, the committee would recommence to finalize the report, essentially. That way we wouldn't be.... It would basically have the same effect, other than not putting ourselves under the gun where we end up with a 12-hour-long meeting again or something, if it's required. One would hope not, of course, but....

That's one thing.

The second would be that I still don't think it addresses the concern that was raised by Mr. Duncan. I don't believe he is here now, but I certainly sympathize with that school of thought, which is essentially that what we're doing is making recommendations in June, or, in this case, maybe early July, for something that is then two and a half months off. With the way the situation evolves, we may find that we want to consider an interim report and then come back and revisit it for some discussion late in August or the first week of September to address where we are at that point and potentially make new recommendations, change existing ones, drop some of them or whatever the case may be. It really doesn't address that.

I don't know that we have to have a motion to do that. I don't know how that needs to be done, but those would be my two thoughts. We can do the first part of it in that manner. Then for the second part, I don't know what to suggest in terms of how to address that, but we probably should have a provision. Probably the

easiest thing to do is to indicate that this would be an interim report and we would have a chance to revisit it when the time is appropriate, whether that is in late August or early September, whatever it might be.

• (1415)

**The Chair:** At this point, after tomorrow.... A couple of the points were about the witnesses. We have exhausted the witnesses we had already requested and all the parties had put forward, so that witness list has been exhausted.

From what we heard from Andre, we will have the complete, finalized draft report by June 18. So, by June 18, we will have a translated, full draft report that includes up to tomorrow.

I have a drafted motion that the clerk has helped draft. We will need to have something to ask for if we don't meet our current deadline, and I need to get that in as soon as possible. The rest is up to when you think that should be.

There are some hands up. We have Ms. Blaney, Mr. Gerretsen and then Mr. Richards again.

**Ms. Rachel Blaney:** Thank you, Chair.

First of all, thank you for clarifying. That was the question I was going to ask, whether there are any outstanding witnesses whom time has prevented us from seeing. It sounds as though that is not the case.

My one concern.... I agree; I would like to set a date. It's important for the House to know when we're going to have this completed. I do agree with Mr. Richards, if there is a way for us to come back at the end of August or the beginning of September to look at what has happened. I know I'll be watching closely what's happening in British Columbia, because of course they're going to start going back to their legislature and doing it in a hybrid model towards the end of June. It would be good for us to have an opportunity to reflect on anything we've seen. I encourage us to consider that seriously.

Maybe the following week, July 15 or 17.... I say that hoping we can meet the week of July 10 but then give ourselves time at the end to get the final reports done, to have them tabled. I just don't want to see us rushing again, the day after the night. I just think about the last time. We were trying to get our report done and then get it translated and submitted. That was a very short timeline, so I'm especially thinking of that.

That's my sense of the conversation at this point. I look forward to hearing from other people.

**The Chair:** That sounds fair. There's probably a way the committee can put a report back with its recommendations, and also perhaps ask for that review mechanism or further input, or whatever it is that the committee desires, to provide feedback to the House of Commons again on the issue.

We have Mr. Gerretsen, and then Mr. Richards.

**Mr. Mark Gerretsen:** Forty minutes ago, we had no problem imposing a strict deadline on the bureaucrats to produce information and on translation to work over the weekend to translate a contract and any other contracts. It's entirely fair that we put a deadline on ourselves, create a deadline for ourselves and work towards that.

We're willing to say that June 23 or June 18, whenever the original deadline was, is a little tight.

**The Chair:** It was June 23.

**Mr. Mark Gerretsen:** June 23 is a little tight, so let's work to find another date. By no means should we be setting ourselves up in a position to say, "Well, if we can't make it, then I guess we'll go a little longer," when 40 minutes ago we basically told people on the Hill they had to work over the weekend. That's the reality of what we just did.

With that, I move that we ask for an extension to July 10.

**The Chair:** Mr. Richards.

**Mr. Blake Richards:** Chair, there are a couple of things.

First of all, you indicated that we'd exhausted the witness list. I'll make a couple of points to that.

There are a couple of ways that a witness list can be exhausted. One of them can be that every witness who desired to be heard was heard. The other way could be, and I suspect it's probably the case in this scenario, that when we're rushed, as we were, they were offered a certain time or maybe weren't available during this period of a couple of weeks that they had. They would have liked to have the chance but just didn't get that chance because of the rushed timeline. We might find that, if we have more time, there might be other witnesses who wish to be heard.

The second point to that is that parties were all encouraged to submit short lists because we were rushed in terms of time. There might be other witnesses people wished to suggest but chose not to because they didn't have the time and had to prioritize. To say that we wouldn't have other witnesses might not necessarily be accurate.

Given that we would then have—

• (1420)

**The Chair:** We have to empty the room. We're running out of time. This is why I was hoping that on Wednesday we could have had a one-hour committee business meeting, but at that time the committee didn't really feel that we would need a whole lot of time on this issue. It seems as though we do.

We have to clear the room, so we have to set aside another time for committee business. I have to figure that out and set that.

Justin.

**The Clerk:** In terms of additional time, we do have a witness tomorrow for a one-hour meeting. We could put on the meeting notice another opportunity for committee business. It would again be fairly brief.

Seeing as the committee is moving towards an idea of some type of extension, next Tuesday, June 16, we will have a full three-hour meeting and there could be an opportunity right off the top, at the

beginning of the meeting, for some additional committee business. If tomorrow's opportunity doesn't allow you to finish off the discussion and reach a decision, there might be an opportunity at the beginning of the Tuesday meeting to do that. There would still be a chunk of time in the balance of that meeting, if that is what the committee ultimately wants to do, to start in on at least a portion of the draft report as Andre currently has it.

**The Chair:** Mr. Gerretsen had moved a date. What can we do with that?

Is your point of order on what I'm just about to bring up?

**Mr. Mark Gerretsen:** No, I want to make sure I understand correctly from a procedural perspective.

If we don't end up asking for an extension, we're ultimately stuck with June 23. Is that correct?

**The Chair:** Yes.

**The Clerk:** Madam Chair, I could provide some clarity on that.

Essentially, the House motion of May 26 was a motion of instruction asking the committee to do a study on possible Standing Orders changes, incremental steps towards a hybrid Parliament, including remote voting. They had a reporting deadline of June 23 in that. The committee would be under some sort of obligation to report something back by June 23.

As I've indicated before, the nature of that report could be a recommendation to extend the deadline to some future point, for example. That's why ultimately the committee needs a specific hard deadline to make a determination on that. Whether it's July 10 or some other date down the road, there would be a need to do that. If the committee makes that type of decision, that could be the report that gets sent back to the Clerk of the House.

Of course, before a deadline can be made formal or official, the House needs to concur in it. Because we don't have the sittings in the usual way where a motion can be moved for a concurrence to the committee report during routine proceedings, some other mechanism would need to be in place that would permit the House to essentially give its approval to your recommendation to move the reporting deadline to some other date.

There are different ways of doing that. Special motions have been done in the House before, and we've seen that since the beginning of the pandemic. It could be done that way. There is a special provision from one of those motions, from April 23, where if the four House leaders of the recognized parties agree to a recommendation in a PROC report, such as a recommendation to extend the deadline, that could give effect to it as well. Simply your deciding to move it to another date does not necessarily guarantee that a new deadline will be officially made or officially set.

The first step, obviously, is to make a decision, if that is what you want, to ask for a deadline extension, and then of course determine what that specific date would be. Whether it's soon or whether it's later, that's up to you.



**The Chair:** Is that something that can be decided by majority vote, Justin, or do we need consensus on it?

• (1425)

**Hon. Omar Alhabra:** Madam Chair, we have a motion on the table. Can we vote before we leave the room?

**The Chair:** That's what I'm asking for.

Is that a votable motion?

**Mr. Blake Richards:** I have a point of order.

**The Chair:** Mr. Richards.

**Mr. Blake Richards:** I had the floor.

I'm not comfortable we're in a spot where voting on this is appropriate. There was still discussion being had. If we're now being told we're able to continue to meet, I'd like to continue the discussion, if we can. We'll have to set aside another time, as you've indicated.

The second part of the point of order is this. You indicated there's been some allusion to a meeting tomorrow. No one on my side, among the Conservative opposition, was aware of the meeting tomorrow. No one knows what the business would be. Can you fill us in on what happened there and how that came to be?

**The Chair:** This was discussed at the last meeting, that we had a one-hour time slot available. We asked some of the international witnesses who had indicated... As you mentioned before, some witnesses indicated they were not interested, and others indicated they were interested, except the previous time was not doable for them. We once again went back to those witnesses to see if they'd

still like to appear. We have one for the time slot tomorrow, and the rest of the time we can dedicate to committee time.

**The Clerk:** Madam Chair, the meeting notice for tomorrow will be published after today's meeting. It should be coming out in the next hour or so.

**The Chair:** The time slot would be 11 to 12.

**The Clerk:** That's correct.

**Hon. Omar Alhabra:** Can we have a vote, please?

**Mr. Blake Richards:** I have a point of order, Madam Chair.

No, that's not possible. I have the floor, and I think there is still a discussion we need to have. I have some other ideas on how we might be able to [*Inaudible—Editor*], and if we have time for that discussion, I'd love to continue to share them.

**The Clerk:** Mr. Richards is right. They're on debate right now on that motion.

**Mr. Garnett Genuis:** I'll just note that I have the floor as well. Sorry, I don't have the floor, but I'm on the list.

**The Chair:** All right. Since we're at a point where we cannot vote on the motion right now since debate is ongoing, we will wrap up for today and we will carry on from this point in committee business tomorrow.

See you tomorrow at 11 o'clock.

Thank you.

---





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

---

### SPEAKER'S PERMISSION

---

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

---

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

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

---

### PERMISSION DU PRÉSIDENT

---

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

---

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