HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

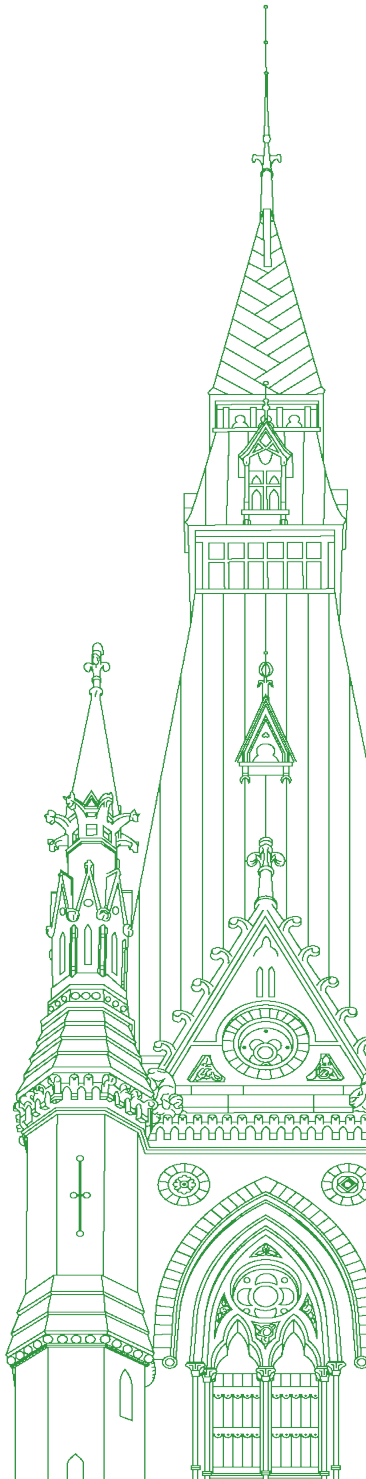
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 040

Tuesday, June 2, 2026



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Tuesday, June 2, 2026

● (1535)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): Good afternoon, everyone.

I call this meeting to order. Welcome to meeting number 40 of the House of Commons Standing Committee on Public Safety and National Security.

Pursuant to the House of Commons order of reference of April 20, 2026, and the motion we adopted on April 30, 2026, we are meeting to study Bill C-22, An Act respecting lawful access.

I would like to begin by welcoming our three witnesses. First, we have Christiane Saad, from the Canadian Bar Association. Second, we are hearing from Alexander Surgenor, from the Canadian Constitution Foundation. Third, Matthew Hatfield, from OpenMedia, is participating by video conference.

Welcome, everyone. You each have five minutes for your opening remarks.

We'll start with you, Ms. Saad.

Christiane Saad (Chair, Privacy and Access Law Section, Canadian Bar Associaton): Thank you very much, Mr. Chair.

[*English*]

Good afternoon, honourable members of the committee.

Thank you for the opportunity to appear today on behalf of the Canadian Bar Association as chair of the privacy and access to information law section, which, with the criminal justice section and the anti-corruption team, has studied Bill C-22. We acknowledge the improvements to the bill from earlier versions, but significant concerns remain.

The CBA notes four critical gaps, but let me begin with the structure. Bill C-22 bundles two different regimes under one banner. These deserve to be debated as separate bills so neither escapes proper scrutiny.

The first gap is the absence of evidence of necessity. When government expands its power into private lives, the burden is on it to show that the expansion is necessary. The government has not demonstrated that current laws hinder investigations. Both the CSIS Act and the Criminal Code already provide for assistance orders with judicial oversight for technical capabilities. Without evidence that these tools are insufficient, expanding powers is premature. In addition, three of the Five Eyes countries mentioned have no constitutional protection against unreasonable searches and seizures. Canada does, so section 8 of the charter must remain front of mind.

The second is that Bill C-22 dramatically expands lawful access power. More parties could demand access, more information could be compelled, technical capacity requirements would be broadened and more entities would be subject to them, while judicial discretion would be reduced. This expansion has lacked adequate consultation with key stakeholders for feasibility, impact and proportionality.

The third gap is the lack of safeguards. In part 1, the bill creates the new “subscriber information” production order on the lowest threshold that our legal system recognizes—mere reasonable suspicion—yet this order compels all subscriber information a provider holds, potentially reaching what the Supreme Court calls “a biographical core”. That definition should be narrowed to information that simply identifies a subscriber.

We are equally troubled by the voluntary disclosure provisions, which appear misaligned with the court's rulings in the Spencer and Bykovets cases, and by non-disclosure orders that can last for a full year. The CBA recommends reducing this to 90 days with court approval required for extensions.

The new confirmation of service demand power allows a peace officer to demand confirmation without judicial authorization and mandates a 24-hour response time. This timeline is unrealistic, especially for smaller providers, and the CBA recommends extending it to 48 or 72 hours except in genuine emergencies.

Part 2 concerns us the most. This new act would require ESPs to build capacity for lawful access, which in plain terms would mean building back doors. These access points would become magnets for hackers. Examples from other jurisdictions show that the equivalent law created vulnerabilities that foreign actors exploited to steal data.

The issue of metadata is even more critical. Although one proposed section would impose some limits on the nature of the data retained, it is well known that the metadata includes sensitive information, and in this context, it can also include location data.

Beyond that, part 2 effectively deputizes companies as surveillance arms of the state while shifting investigative costs to the private sector without compensation and without judicial overview. The CBA recommends that these ministerial orders be removed, that the definition of “systemic vulnerability” be strengthened to expressly protect encryption and that the government bear costs and risks related to these.

As for the fourth gap, the CBA sections believe that Bill C-22 risks violating section 8 of the charter.

The CBA is not opposed to supporting law enforcement; however, the CBA opposes expanding state surveillance powers without evidence of necessity, without adequate safeguards and without sufficient judicial oversight. Further details are in our original submission.

Thank you for your consideration.

● (1540)

[*Translation*]

The Chair: Thank you, Ms. Saad.

I now give the floor to Alexander Surgenor for five minutes.

[*English*]

Alexander Surgenor (Counsel, Canadian Constitution Foundation): Good afternoon, Mr. Chair.

My name is Alexander Surgenor. I'm counsel with the Canadian Constitution Foundation. We are a non-partisan, donor-funded legal charity. Our work consists of education and advocacy on matters pertaining to civil liberties, the rule of law and our constitutional order more generally. This is my first time appearing, so I thank you for the invitation.

Our concern with this bill is long-standing. It dates back to really the progenitor bill, Bill C-2. While we're pleased with the evolution there and the modest amendments and changes that followed, we remain concerned, and in fact even more concerned, about Bill C-22. That's why I'm here. I don't mean to be hyperbolic, but truly it's difficult to escape the inference that Bill C-22 would establish a pretty powerful regime of surveillance and constitute a pretty severe invasion into the privacy of everyday Canadians. Our concerns are fundamentally about the intrusiveness, the vulnerability and the overall secrecy that this bill envisions.

Allow me to identify exactly what I understand this bill to require. So-called core providers may be ordered to develop, test and maintain technical capabilities for extracting information, in particular computer data. I'll get to that in a moment. This would be achieved in part by installing, using and maintaining prolonged and continued access to perhaps any given device. The concern here, of course, is that it's not just so-called core providers. It's the fact that electronic service providers, carrying an enormously broad definition, could also be required, following a ministerial order, to undertake those same acts that the so-called core providers are. Very quickly, an electronic service provider could also become a core provider. There's no reassurance to be had in really defining those two terms differently. They're one and the same, and they would be quite quickly.

What is an electronic service provider? It is any entity that provides business in this country, or conducts a portion of its business in this country, through electronic channels, be it through the Internet or perhaps through software that's installed and kept locally on a device. Internet connectivity is relevant in that case.

Now, at the heart of it here, and really the pith of it, is the concern about metadata. Metadata is information about information. While the context of a text message might not be accessible, the fact that a text message, as an example, was sent could be accessed. To whom, when, how—all of that is fair game. The fact that a phone was used on the Hill in Ottawa, two days later in a library in Corner Brook, and then on another day finds itself in a hotel room in Saskatoon—that is all fair game. With this bill, we can monitor that, keep track of that and follow that.

In other words, the entirely innocuous and inherently private comings and goings of ordinary citizens are up for grabs. Up to a year's worth of movement, communication, work and ordinary life would be preserved for review while the private citizen, of course, is kept completely oblivious as to this occurring or not. Though the bill says no such order would be made if it would introduce a systemic vulnerability, I'm not particularly sanguine about that. The notion that only the good guys will have access to this flies in the face of examples from our peer nations in the Five Eyes that have suffered data breaches of exactly the sort that would constitute a systemic vulnerability.

If the aim is to better investigate criminal activity—I have some knowledge of this, having worked as a criminal defence lawyer and having seen both sides of this—it's unclear to me why the proposed powers have to be so broad to capture basically every device in this country. The CCF would gently remind everyone of the terms “public official” and “private citizen” and the key distinction there.

The importance of privacy cannot be overstated. Privacy is about dignity and autonomy. These are the predicates of a free society. To have a truly free society, we must be free to make our choices without the sense of being monitored—and, of course, not even knowing that we're being monitored.

I see that I'm at time. Once again, I thank you for hearing our concerns and inviting me to participate in this critically important discussion.

● (1545)

[*Translation*]

The Chair: Thank you, Mr. Surgenor.

I now give the floor to Mr. Hatfield, from OpenMedia.

[*English*]

Matthew Hatfield (Executive Director, OpenMedia): Good afternoon.

I'm Matt Hatfield. I'm the executive director of OpenMedia, a grassroots community of 230,000 people in Canada who work together for an open, accessible and surveillance-free Internet. I'm joining you from the unceded land of the Tsawout on Salt Spring Island in B.C.

Do not let the public safety minister convince you that limited amendments will fix Bill C-22. They will not. Nothing short of striking the majority of part 2 will protect Canadian privacy.

The government's current approach is an enormous own goal against our economy and our security, and you are the only people who can stop it. I won't repeat the facts you've heard from Professors Diab and Geist and Apple, Meta and others. I'll use my time to explain why light amendments cannot do the job of making this bill safe.

In recent weeks, the minister has said the government will amend Bill C-22 to bring it in line with our allies' lawful access like America's CALEA, so let's compare. Bill C-22 can require telecom companies, online services and even hardware manufacturers to let the government install surveillance equipment on their platforms and to retain a year of metadata on every person in Canada. That isn't catching us up to CALEA. The two aren't even in the same league.

CALEA covers only telecom companies and requires no metadata retention: nothing approaching a year's data on everyone by default. Of the Five Eyes, only Australia mandates metadata retention, and there it's deeply controversial and is being reformed. I think we need to bear in mind, taking a step back, that in this threat environment we're entering, CALEA is not a success. CALEA has been in effect since the 1990s, but in recent years, the back doors required by CALEA are increasingly a key entry point for foreign hackers to compromise U.S. privacy.

In 2024, Chinese state hackers used it to compromise the systems of America's largest telecoms, affecting more than a million people. Just this February, the FBI found that CALEA's back doors had led to breaches in their systems and reported it to Congress as a major security failure.

We aren't catching up to a working global standard here. We're leapfrogging well beyond what any of our allies have done, creating a more vulnerable version of a system that's failing other governments.

What about the minister's promise that selective amendments can fix the bill?

The security and legal experts you've heard from have been clear: This bill will not protect encryption in any way that matters. The government's promise is to provide a narrow technical protection that Bill C-22 won't force a company to break encryption, but breaking encryption as a standard and defeating it are not the same thing.

A working lock is no protection if you're required by law to leave the door open. Bill C-22's capability orders can compel a provider to build in access to information before it's encrypted or while it's temporarily decrypted: at the device level, within the software or as data is being handled. None of that breaks encryption as a standard. All of it circumvents the protection that encryption is supposed to provide. That's a foundational problem of Bill C-22, not a simple definitional problem to fix.

In fact, this bill, as written, makes sure that none of its definitions can actually protect Canadian rights. Much is made of the difference between an electronic service provider and a core electronic service provider, with the strongest default obligations on core providers, although the government of course will decide who a core provider is later by regulation, but proposed subsection 7(1) lets the minister impose any obligation that a core provider faces on any service provider.

Because these orders have no gazetting requirement, counterintuitively every invasive requirement a core provider faces can be applied to any provider with less public scrutiny. In that same logic, maximal flexibility—ineffective-by-design safeguards—governs the definition of systemic vulnerability. That definition today isn't good enough, but even a strengthened good-faith version won't fix Bill C-22, because proposed paragraph 47(1)(c) explicitly grants cabinet the regulatory power to reinterpret any term in the bill.

As the case for Bill C-22 has crumbled, the minister has claimed that opposition is driven by foreign big-tech firms attacking Canadian sovereignty. That's plainly not true. Canadian tech success stories like Windscribe and Shopify have rallied against this broken bill as strongly as anyone.

OpenMedia's community has sent nearly 25,000 messages to MPs opposing Bill C-22 and Bill C-2 before it and has helped to rally more than 300 organizations against Bill C-2's privacy provisions. We don't take a dollar from big tech. Our budget comes from small donations from ordinary Canadians. The truth is that big-tech firms were late to this conversation, and it was ordinary Canadians who sounded the alarm from day one.

Now, the minister has said the government wants to have a filing cabinet of every Canadians' metadata ready for law enforcement when they need it. To that, I say that democracies do not keep a filing cabinet of every citizen's sensitive information in case it's useful to spies or police.

This process has been pushed so quickly that the system is not keeping up. We submitted our brief more than two weeks ago, on May 15, yet due to the sheer volume of input you've received, I learned today that committee members have not yet received it.

● (1550)

This is the symptom of a rushed, under-resourced process for a bill that has massive stakes. On behalf of our community, I urge you to take the time to receive and review all public evidence and to thoroughly reform or abandon part 2 of Bill C-22 before it moves forward.

Thank you. I look forward to your questions.

The Chair: Thank you, Mr. Hatfield.

Let's turn to MP Caputo.

Jacques Ramsay (La Prairie—Atateken, Lib.): Mr. Chair, I have a point of order.

Ms. Saad has alluded to a memoir being presented. It may be my mistake, but I can't find it.

[*Translation*]

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): I have it.

[*English*]

Jacques Ramsay: Is it in the binder?

[*Translation*]

Claude DeBellefeuille: We received it in both official languages. Did you not receive it?

Jacques Ramsay: Are you talking about the Canadian Bar Association's brief?

Claude DeBellefeuille: I made a mistake; I have the one from the Barreau du Québec.

Christiane Saad: We sent you our brief last week in French and English.

The Chair: According to the information I have, the French and English versions of the Canadian Bar Association's brief have indeed been submitted, but the House's translation service has to validate both versions. If I understand correctly, the validation process is still under way.

That said, I'll give the floor to Mr. Caputo for six minutes.

[*English*]

Frank Caputo (Kamloops—Thompson—Nicola, CPC): I'm sorry. I'm going to speak about this in my time because I think it's very important to speak about it.

Mr. Hatfield, I was going to ask questions about section 8, search and seizure and de facto seizures.

Just so that I'm clear, Mr. Chair, is it the policy, when a brief is submitted, that translation has to review it, even though it is translated already? Do I have that right?

The Chair: [*Inaudible—Editor*]

Frank Caputo: Okay.

In the interim, though, prior to translation, can it not be disseminated, and then the translated version, the authenticated version...?

I'm trying to choose my words carefully, and I'm not trying to cast aspersions or blame. If a brief was submitted two weeks ago by OpenMedia, I guess I'm asking, what was the delay from two weeks ago to now?

The Chair: Exceptionally, I can ask the clerk to provide guidance as to what happened.

The Clerk of the Committee (Paul Cardegna): With regard to OpenMedia, we received their brief, and like a lot of others that we have received, it is in translation. As I explained to Mr. Hatfield earlier today, we are dealing with a large number of documents that have been submitted. Unfortunately, we are not the only committee drawing on translation resources. This has caused longer than expected or anticipated delays, which—though unfortunate—is not something that is in the purview of the committee to deal with at this time.

With regard to documents submitted in French and English, this is the rule of the committee, established by the committee. Any document that doesn't come from an MP's office, from a department or from the House of Commons and that is submitted in both official languages has to be sent to the Translation Bureau for linguistic review. Then we fall back into the same issue: The translation bureau has an enormous amount of work to do, which is causing longer than anticipated delays.

Thank you.

Frank Caputo: When are amendments due?

The Chair: The were due yesterday.

Frank Caputo: I guess I'm a bit concerned because we don't know what we don't know as committee members. By that I mean I don't know how many briefs are outstanding. We have submitted our amendments. Obviously, that's on behalf of the Conservative Party. I have to ensure that His Majesty's loyal opposition is properly represented.

We know of at least two that are outstanding, and we wouldn't know about this if we were not having this meeting. It seems to me that the appropriate remedy should be to reopen the deadline for amendments. I'm not going to give away our work product, as a lawyer, but I will say that my staff, who have done an excellent job, go through these briefs; they do review them. They do look at amendments, and they do cross-reference them to the point where—I'm not telling tales out of school—there are 70 amendments we've looked at.

Mr. Chair, this is a problem, and I'm not sure how we deal with it. With the greatest of respect—and I'm not trying to throw anybody under the bus—if there are not enough resources for translation, and the government wants to have its legislative agenda passed, then you can't exactly have your cake and eat it too by saying, “Get this done, but we're not going to allocate the resources to get the translation done.”

I will resume my six minutes, if there's anything left. I'm not sure if the clerk can tell us this. What briefs are currently in that translation line, if you will? Does that make sense? What don't we have that has been submitted?

● (1555)

The Chair: Let me summarize on three different points.

First, as we know from experience, the submission of briefs is a continual process. There were briefs several weeks ago. There were briefs submitted a few days ago. I suspect there could be briefs submitted today. There will be briefs and views submitted over a continuous time period.

The second thing is that the translation bureau, as the clerk mentioned earlier, proceeds in terms of priority. It does the work most professionally, and it does what it can to assist the members of this committee.

The third thing is that we have already committed to an agenda. Today is the last day for witnesses and we have decided that we will be moving to clause-by-clause work on Thursday. As we know, between now and Thursday there will be more work ongoing.

Having said that, I think there is more time for you, Mr. Caputo, to continue your intervention.

Frank Caputo: I have to register for the record, Mr. Chair, that we still don't know what briefs are outstanding. What I would like is—and I would hope that all colleagues around the table would say this—before we move to clause-by-clause....

Amendments were already due. We know right now of two briefs that we haven't seen yet. Are there more? I think the committee has a right to know that.

The Chair: There are possibly more, MP Caputo, but unfortunately at some point we have to stop hearing witnesses and considering additional briefs. Otherwise, this process is never going to end.

Frank Caputo: With the greatest respect, Mr. Chair, I would agree with you that if the brief came in yesterday, the day before or even Friday.... These are briefs that came in two weeks ago. Yes, we do have to draw a line. The question is, when should that line be drawn? If a brief is submitted well in advance of the period in which we are considering amendments, I think we are bordering on a privilege issue.

I would shudder to think that anybody around this table thinks that.... This is Parliament, for goodness' sake. We shouldn't be waiting two weeks without even knowing if something is there. It doesn't feel right, to be very candid, that briefs are sitting in the queue, we don't know they're sitting in the queue and we're putting forward amendments. The only alternative is then to table-drop amendments after the fact.

Perhaps I'll have something more official to say. I'm just thinking out loud here. The fact that I'm not getting point of ordered speaks volumes, although I might get one now.

● (1600)

[*Translation*]

The Chair: The House of Commons, like any other organization, has limited resources. All committees face the same circumstances and constraints. Our committee is no exception.

We work with the resources allocated to us, and that's why, since time is also a scarce resource, you have about one minute remaining in your speaking time, if you want to continue speaking.

[*English*]

Frank Caputo: With that one minute, let's talk about what we do know.

Ms. Saad, I'm a law nerd—full disclosure. You spoke about section 8 of the charter being engaged. My reading of the bill is that the requirement for data retention is on the third party, those who are covered by the bill, and a warrant is then required to access the data.

Can you connect the dots for me, please? I'll ask your colleague to do this as well, in terms of whether a warrant is required. I believe, prima facie, that the search is legal if a warrant is required. Can you help us out there on a charter breach? Am I making any sense here?

Christiane Saad: Our analysis for the charter part is that by retaining all this data, and eventually the metadata, for such a long time, we have so much information retained on people. The fact that we are requiring so much subscriber information—and not just who is the subscriber—may include this breach of the charter because it's way beyond the reasonable suspicion that usually is required.

Frank Caputo: Okay, so it's the volume of the data—

Christiane Saad: It's the volume of the data and the type of data as well.

Frank Caputo: —and it's the fact that the government is compelling that data to be kept. I don't want to put words in your mouth; I just want to make sure—

Christiane Saad: Yes. Also, the type of data is problematic in this case as well.

Frank Caputo: Mr. Surgenor, do you share that view?

The Chair: Unfortunately, MP Caputo, that's all the time we have for now, but there might be an opportunity to get back to you shortly.

[*Translation*]

Ms. Dandurand, you have the floor for six minutes.

Marianne Dandurand (Compton—Stanstead, Lib.): Thank you very much, Mr. Chair.

I would like to reinforce the point you made a little earlier. Our colleague across the way talked a lot about the lack of time. I would like to remind him that we have adopted motions in recent meetings to proceed to clause-by-clause consideration. We have added an extra day to hear from more witnesses. We have had enough time to propose amendments. I think it's important to respect the committee's desire to continue the study as agreed so that, following this testimony, we can finally move on to the clause-by-clause consideration of the bill.

So thank you, Mr. Chair, for making that point. I wanted to reinforce that position. We have other business to attend to in committee, and we must continue our work.

Now I'd like to turn to the witnesses, whom I thank for joining us.

My question is for both the Canadian Constitution Foundation and OpenMedia. We've heard a great deal about their concerns regarding this bill, but I'd really like to go back to the very beginning, to this bill's actual purpose.

I would like to ask these two witnesses if we can at least agree on one thing—that police forces today are facing real challenges related to encryption and digital communications when investigating child sexual exploitation, organized crime and terrorism, among other issues.

As a starting point, can we agree on that?

[*English*]

Alexander Surgenor: Thank you, Madame Dandurand.

I lament having discontinued my French after high school, although it was my best subject. I'm certainly very rusty now.

I don't think anybody would deny there are very serious complications in an ever-connected world. That goes without saying. Again, I think I do bring a unique perspective, having actually represented individuals charged with those very crimes.

I'm not celebrating the fact those crimes occurred, of course not. What I am hoping to point out, as my colleague Ms. Saad alluded to, is that there adequate means already exist to investigate crime. I've seen it. I've reviewed the disclosures in court. I've run trials and lost trials because the evidence was robust enough and the police were clearly able to do what that they needed to do. Granted, lamentably, there are more cases out there, and they need to be investigated.

The concern, of course, is really with the scope and the breadth of the search. No one present here today would ever suggest that we need to curtail what already exists. It's more a question of limiting the half-conscious expansion of power and inflation of authority where I think there hasn't been compelling evidence to suggest this is imminently and eminently required at this time.

I hope I've answered your question in a not-too-roundabout away.

● (1605)

[*Translation*]

Marianne Dandurand: That's fine.

I'd like to ask Mr. Hatfield the same question.

[*English*]

Matthew Hatfield: We do not put cameras and microphones in the home of every Canadian, even though that would be useful for investigating many serious crimes. This bill is doing a version of that—certainly on the metadata, and arguably on other data as well—to every online service. Yes, there are serious crimes that you're mentioning. A version of part 1 could be useful to the police in investigating them, but part 2 is well beyond that and way out of line.

[*Translation*]

Marianne Dandurand: My next question is for both of you.

Do you think it's possible to have a modern lawful access regime while maintaining privacy protections, or do you think these objectives are absolutely incompatible?

[*English*]

Matthew Hatfield: Again, a version of part 1, with appropriate amendments, could accomplish some of that, but part 2 is not necessary, and goes well beyond what is helpful.

[*Translation*]

Marianne Dandurand: What do you think, Mr. Surgenor?

[*English*]

Alexander Surgenor: Yes, I'm just thinking about that. I'm no parliamentarian, so the actual process here is somewhat foreign to me, notwithstanding the fact that I, too, am a lawyer like many present.

I would just say that what struck me—and I think I share a similar perspective as Mr. Hatfield—is the imbalance between the first part of the bill and the second. In fact, I remember communicating with colleagues who are eminently more qualified than I—and yet here I am—who helped shed some light on the fact that the first part of the bill is what I would expect and want to see in a proposed bill. That is to say, it's a thoughtful and progressive evolution of what we're seeking to achieve here, which is supporting law enforcement and bolstering the tools that police have.

However, I would say there is a way to do that which doesn't require such a leap forward. I think there's a kind of internal coherence—or at least there should be—in the process both in making law and in investigating crime, where one must lead to two, two must lead to three, and so forth. I'm not particularly convinced that we live in a moment that is any more challenging than any other moment that came before it. I think if you were to rewind the clock to any particular time, the difficulties people faced were the difficulties they faced, and the tools—

The Chair: I'm sorry to interrupt, Mr. Surgenor, and as always it's with great regret that I do that, but we now need to turn to Madame de Bellefeuille for six minutes, please.

[*Translation*]

Claude DeBellefeuille: Thank you, Mr. Chair.

First of all, I just want to echo Mr. Caputo's remarks. I think everyone around this table will agree that all parties have decided to work together to conduct a rigorous study without filibustering, as this is truly a bill that deserves the committee's full attention.

However, when a schedule was proposed to us, we were never told that we would not have access to translation services to enable us to read the briefs. It seems a bit odd to tell the whole world that Canada can't afford to translate briefs—like the one from the Canadian Bar Association, for example—within two weeks. In my opinion, this is unacceptable. I understand that resources are limited, but when we want to speed things up to study an important bill like Bill C-22, we need to make the necessary arrangements. It's a matter of prioritization. Not every committee is studying at an important bill like Bill C-22.

In any case, I find what's happening now unacceptable and quite embarrassing. You will understand that I am a Quebecker and that I want Quebec to become a country, but if I were a Canadian, I would be very embarrassed to tell the entire world that we do not have the capacity to translate documents for the study of a bill that police officers have been waiting for for 30 years.

Ms. Saad, I'm not sure if I understood something you said correctly. I'd like to clarify this with you. You implied that the bill could be split. We could pass the first part of Bill C-22, then discuss and debate part 2 in greater depth—the part that seems less viable or that appears to have less support from the public, civil society and even a professional association like yours. Did I understand correctly that you encouraged us to consider this approach, which could rally more support for part 1, since part 2 seems to pose more problems?

● (1610)

Christiane Saad: This is precisely one of the Canadian Bar Association's recommendations, given that the objectives of the two parts are complementary but truly distinct. So, yes, that is really an approach we recommend.

Claude DeBellefeuille: It's true that we are under a lot of pressure. All the police associations are writing to us. The only witnesses who support Bill C-22 in its current form are the police forces. Obviously, they need a tool. As Ms. Dandurand said, I think we need to modernize the lawful access regime and provide police officers with better tools.

However, it seems like a monumental task, because all the other witnesses oppose it. Some people are almost totally opposed to this bill and are at one end of the spectrum, much like OpenMedia, while police officers support this bill and are at the other end of the spectrum. For our part, we are trying to figure out how to make the bill acceptable. I understand that splitting the bill would be one way to speed up the process, and I feel that, this way, part 1 would be passed quickly.

Personally, I don't have much technical or IT knowledge. Ms. Saad, you are a lawyer and you rely on statutory provisions, the Canadian Charter of Rights and Freedoms, court rulings and so on, and you are concerned about privacy protection. There's one thing I often say: We like to compare ourselves to other countries and tell ourselves we are lagging, but, in my opinion, the countries we are comparing ourselves to aren't good examples. For example, if we compare ourselves to the United States, we need to realize that there's no oversight there and it's a bit like the wild west. The United Kingdom allows for a significant invasion of privacy. So, I dislike it when people compare Canada to countries that do not necessarily have good privacy practices.

My question is for you, Mr. Hatfield.

Could you tell us what scares you the most, from a technical standpoint?

The bill could include a ban on circumventing encryption and a ban on breaching end-to-end encryption. It could be written in black and white. Would that be enough for you, or would there still be ways to circumvent the intent even if it were written in black and white?

If there were an amendment proposing this ban, would that reassure you?

[*English*]

Matthew Hatfield: It's not strictly necessary to break encryption. That was a point I was trying to make in my remarks.

The concern is that by having the power to install devices into systems, there are many ways you can get around encryption without breaking the technical standard. Adjusting the order-making power so it could never have the effect of circumventing encryption, that would do some work on that front.

Also, we're extremely concerned about this metadata retention requirement. There's just nothing like this in any other comparable democracy. It needs to go entirely.

[*Translation*]

Claude DeBellefeuille: The bill proposes a metadata retention period of up to one year. If a 90-day period were proposed, would that be more reassuring to you? Would you be comfortable with a 90-day period?

[*English*]

Matthew Hatfield: We'd not be comfortable. It's still incredibly valuable and incredibly personal data.

It's every person you've spoken with for 90 days and every place you've gone to for 90 days. That's actually an enormous picture of your life. Not only is that a bit concerning to hand to law enforcement, but if and when—and when is likely—that data is compromised, it's a huge amount of personal information in the hands of bad actors and on the dark web, potentially permanently.

[*Translation*]

Claude DeBellefeuille: Mr. Hatfield, it takes time to gather the documents needed for an investigation. Furthermore, we would certainly like to see malicious individuals arrested. Don't you think it's unreasonable to say that there should be no data retention at all?

● (1615)

[*English*]

Matthew Hatfield: There's a reason that very few of our allies do this. It's constitutionally questionable. It's the fact that it creates a pre-emptive collection of data from many millions of Canadians at once on every service that is scoped in.

We don't normally do surveillance of everyone just in case it proves useful. Normally, the process would be that if there's a warranted crime occurring, then perhaps you might start surveillance. That's how the traditional system works, and that would be a more appropriate system.

[*Translation*]

The Chair: Thank you very much, Mrs. DeBellefeuille.

Mr. Gill for five minutes.

[*English*]

Sukhman Gill (Abbotsford—South Langley, CPC): Thank you.

This is an open-ended question to all the witnesses here today. Thank you for being here.

Does it feel rushed to you that we don't have enough time to study part 2? Could each of you respond to that, please?

Christiane Saad: I'll respond briefly.

This is one of our conclusions. There are too many pieces, and the risks are too high for all Canadians and all the parties involved. We recommend more consultations with different stakeholders.

Sukhman Gill: Mr. Surgenor.

Alexander Surgenor: I would echo that broadly. Again, I don't know what precisely it takes for parliamentarians to achieve what they need to achieve, but my sense in reviewing the bill is that it's about the sheer scope of words. I'm speaking as a former English major now, but it's about the number of words. I mean this in not too cute a way, but there are many verbs in this bill—"use", "access", "take"—and these are not trivial words. They are extraordinarily broad. They just are.

It's been quite a task to review this bill. I've had to review it countless times, at this point, and at no point have my worries been assuaged. I think much more time is needed just to go through some of these basic definitions.

Sukhman Gill: I agree, 100%. Thank you for that.

Mr. Hatfield, could you please provide a response as well?

Matthew Hatfield: Look, this is the most dangerous surveillance bill I've seen in more than 10 years of doing this work in Canada and even in other democracies. It has not gotten nearly enough time. If we had realized, I guess on a resource limit, that our brief was being held up and wouldn't reach you before you considered amendments, of course we would have gotten it in your hands by another way sooner. Certainly, you need to take more time to assess the weight of evidence here and realize that the weight of evidence is overwhelmingly against proposed part 2.

Sukhman Gill: Yes. It is quite upsetting to be in kind of a dark hole and not have the information we need that is so crucial to the study.

I have one quick question for you, Mr. Hatfield. In an open letter of yours, your company argued that certain aspects of the bill would "create an unprecedented and extraordinarily dangerous surveillance architecture that could impact every digital tool people in Canada depend on every [single] day".

Could you please expand on the specific aspects of Bill C-22 that you believe pose greater risks for Canadians' privacy and cybersecurity, and which amendments would most improve the proposed framework of this?

Matthew Hatfield: This gets back to the definition of "electronic service provider" and how enormously open-ended it is. The government has refused to put clear limits on that. The government, of course, can scope folk in as a core service provider for undefined reasons in the future. The baseline definition of electronic service provider includes basically everyone who handles data. Of course, the minister has the power to issue any of the orders requiring any of the features it requires of a core provider or of a non-core provider in the future.

We continue to realize just how extraordinarily broad this is in scope. Does that mean the minister would abuse it on day one? No, not necessarily—but having it so broad textually is very problematic.

Sukhman Gill: Thank you very much.

I would like to allocate the rest of the time to my colleague Roman Baber.

Roman Baber (York Centre, CPC): This is for the Canadian Bar Association, following up on Mr. Caputo's question on seizure.

The issue is not that a third party is holding on to the metadata. It's the fact that it's holding it by virtue of a government order, effectively. It doesn't matter if a school principal is holding on to the contents of a student's locker by virtue of police direction or government direction. That's a seizure. If a gym is holding on to my gym bag because the cops asked them to, they're an agent of the state, and therefore there is seizure. Am I correct in that respect?

● (1620)

Christiane Saad: Yes.

Roman Baber: To follow up, some people are making the argument that there is no production because the metadata never left the Internet provider, but the production is in the holding. It's already defined because the service provider is ordered to hold it. Effectively, it's defined data and defined information. Am I wrong on that?

Christiane Saad: The problem is not only the holding. It's all the risk from holding all this and the potential access—

Roman Baber: I'm not talking about risk. I'm talking about the law. I'm talking about the fact that by virtue of its being held, defined and filed away, that amounts to the level required to meet a breach of section 8.

Christiane Saad: According to our study, yes, but I need to check—

Roman Baber: Okay. That's the brief—

The Chair: Thank you, MP Baber. That was short, indeed.

MP Sodhi, you have five minutes, please.

Amandeep Sodhi (Brampton Centre, Lib.): Thank you, Mr. Chair.

Thank you to our witnesses for being here today.

Ms. Saad, from a legal standpoint, how do you suggest that we balance the safety and security of Canadians with the concerns your organization has raised?

Christiane Saad: You will receive it eventually, but in our full submission we propose certain amendments, although we highlight many risks, as I mentioned.

Part 2 of the bill is really problematic, and it needs additional amendments to strike this balance that you are referring to.

Amandeep Sodhi: If you're able to, can you elaborate on some of those amendments? We don't have the brief right now.

Christiane Saad: I've mentioned the ministerial orders that we recommend be struck.

Another recommendation is on systemic vulnerability. We recommend an amendment to the definition. We recommend really focusing on and mentioning the encryption part to clearly carve out the encryption. We recommend the following: “Systemic vulnerability” means a vulnerability in an electronic protection that creates substantial risk of confidentiality, integrity, availability of information or services. This is one of the other amendments.

I mentioned the question of the involvement of the electronic service providers, where they are involved without compensation and without holding all the risk. We also recommend that the minister should have to justify, on a per order basis, the need for secrecy associated with these orders. These are some of the recommendations as well.

For inspection powers, we recommend including a threshold of reasonable and probable grounds before designated persons can enter the premises. We elaborate on some of these. As well, for the audits, we recommend that further procedural safeguards be included.

In several sections in our submission, we also highlight the judicial overview and the possibility of appeal and judicial review.

These are some of the recommendations in our submission.

Amandeep Sodhi: Thank you.

The CBA's membership includes a wide variety of people such as Crown prosecutors, police legal advisers and counsel who represent lots of different sectors. Do you believe it's fair to say that the CBA might be divided on the question and topic of lawful access? How was the association's position on Bill C-22 developed?

● (1625)

Christiane Saad: The CBA represents over 40,000 lawyers from all different practice areas from the public and private sectors. All of our submissions are also reviewed by policy committees at the CBA.

For this submission, we worked with the criminal justice section and the privacy and access section. We are not that divided on part 1. We reached a consensus.

Amandeep Sodhi: Would you say that there is a divide?

Christiane Saad: No.

As I said earlier, what you will see in our submission is that we are not divided. This is the opinion of all the sections that worked on the submission, and the CBA approved it as well. We are speaking with one voice.

[*Translation*]

The Chair: Thank you, Ms. Sodhi.

I will now give Mrs. DeBellefeuille the floor for two and a half minutes.

Claude DeBellefeuille: Thank you very much, Mr. Chair.

Ms. Saad, we note that your concerns are virtually identical to those of the Barreau du Québec. It's a shame we did not receive your brief to review your proposed amendments, because we had until last night—or until May 27—to submit them. Of course, we can always propose them on the spot, but that's always more complicated. So, it's unfortunate.

Mr. Surgenor, I'd like you to tell us about other countries. We've been hearing nothing but positive things; however, in recent weeks, some witnesses have told us that we shouldn't compare ourselves too closely to them, because we aren't really that similar. Essentially, in Canada, we have a culture in this regard—or a deep commitment to the protection of privacy.

In your opinion, are there things that other countries do that we shouldn't replicate and that shouldn't be included in the bill?

[*English*]

Alexander Surgenor: Madam, regrettably, I have to inform you that I'm not up to speed on the precise contours of what the other.... I'll use the phrase “Five Eyes”, because that's what it is. It seems that we've heard this from those who have spearheaded this bill: that, really, we're talking about the Five Eyes.

I'm afraid that I just don't have the knowledge about what other countries are doing, but with respect to the culture of privacy, I would suspect that's something that's shared across the Five Eyes. I'm drawing that inference because there's been a robust history of co-operation for many years at this point, but I can't give you a more fulsome answer.

I know that from the Canadian perspective—and I'd like to again highlight the non-partisan character of our organization—our concern is a general one. It's a concern about the sheer overbreadth of this proposed legislation. If criminals are the ones that need to be targeted, there's a way to do that in a more targeted way. That doesn't appear to be the case with this bill. It seems that far too many people who have absolutely no connection to criminal activity would be caught up in this.

I can't speak for our Kiwi, Australian, British or American friends, but I would hope that they're not interested in investigating innocent people. What they're doing precisely, I can't say.

[*Translation*]

Claude DeBellefeuille: Thank you.

The Chair: Thank you, Mrs. DeBellefeuille.

Ms. Kirkland for five minutes.

[*English*]

Rhonda Kirkland (Oshawa, CPC): Thank you, Chair. I appreciate the time.

I have a few questions that I'd like to ask all three witnesses. More than likely, they will just require yes-or-no answers. If there's something very important that you feel you need to add, do let me know.

Throughout the study, we've heard department officials and even the Minister of Public Safety repeatedly say that Bill C-22 is encryption-neutral—that was the word used—and does not create back doors.

Having reviewed the legislation, do you believe those assurances are fully reflected in the text of the bill itself, Mr. Hatfield?

Matthew Hatfield: There's no such thing as encryption-neutral, and this would damage encryption's purpose very severely.

Rhonda Kirkland: Thank you.

Ms. Saad is next.

Christiane Saad: We think they're not.

Rhonda Kirkland: They're not.

Next is Mr. Surgenor.

Alexander Surgenor: I'm sorry. Could you pose the question again?

Rhonda Kirkland: Having reviewed the legislation, do you believe the assurances that Bill C-22 is encryption-neutral are fully reflected in the text of the bill?

Alexander Surgenor: It's hard not to be cynical. As a lawyer, I don't really believe many assurances from anyone, because I can't even trust myself most of the time.

● (1630)

Rhonda Kirkland: Okay. That's fair.

Alexander Surgenor: I think it's quite clear that what's outlined is a not so—

Rhonda Kirkland: It sounds like it's not clear.

Alexander Surgenor: No, let me clarify—my apologies.

The answer to the question is no. It seems like the aim here is to create a path to access.

Rhonda Kirkland: That answers my question. Thank you.

Again, for all three of you, do you believe there's a clear difference between what the minister says the bill is intended to do and what the bill would legally allow or permit a future government to do?

Matthew Hatfield: Yes, very much so. Intentions don't matter. What the text does here is well beyond what the minister has said the purpose is.

Rhonda Kirkland: Thank you.

Ms. Saad is next.

Christiane Saad: We agree.

Rhonda Kirkland: Mr. Surgenor, you're next.

Alexander Surgenor: Yes, I agree. I appreciate Mr. Hatfield's comment about subsequent...or the question, rather, with respect to—

Rhonda Kirkland: Subsequent governments...?

Alexander Surgenor: Exactly. That's because legislation, if not repealed or amended, does tend to take on a life of its own after a time. Maybe the original purpose is forgotten or muddled over time, and that's a concern.

Rhonda Kirkland: That's wonderful. Thank you.

This is the conclusion I'm coming to and I would like to see if you would agree with me. With Bill C-22, the Liberal government is selling Canadians a privacy promise that the actual legislation doesn't deliver as it is written today.

Matthew Hatfield: Yes, I agree. If anything, I'd be stronger than that.

Rhonda Kirkland: Is that fair?

Christiane Saad: I wouldn't phrase it that way, but we have serious concerns in terms of privacy.

Rhonda Kirkland: Thank you.

Alexander Surgenor: I'm sorry. Can the question be asked again?

Rhonda Kirkland: Yes, no problem. Maybe I should go to you first the next time.

It feels like we're being sold a privacy promise that the actual legislation doesn't deliver. Would you agree?

Alexander Surgenor: I don't know about the word “promise”. I just have an issue with the legislation as it currently exists, because I think, as I've said repeatedly, that it's too broad and there are too many entry points.

Rhonda Kirkland: I think you've all said you agree that things are too rushed. We've barely had time to absorb pieces of this bill, let alone all of it. I have significant concerns about that, and I've said that many times. Rushing a bill is not doing it justice and could cause a great deal of harm.

Mr. Surgenor, you talked about metadata being “information about information” that is preserved for review. I appreciate that because I don't know if Canadians really understand what metadata is. Can you clarify what it is—information about information—and why storing metadata could be harmful if it's for every Canadian?

Alexander Surgenor: That is the position that we have: Metadata is information about information. It took some time to wrap my head around that, because you're quite right that it's not exactly clear.

The language of the bill is kind of a thin veneer. As I read it, it's not a great leap to learn, for instance, that device X was communicating with device Y, even if the content of the communication isn't clear, especially given the fact that all sorts of related information is also up for grabs. Presumably, the point of the investigative powers is to gather as much as necessary to positively identify an individual, particularly, to echo Ms. Saad's comment, when we talk about the definition of subscriber information.

Taken together, you have a constellation of information, and that's what the metadata is: device X talking to device Y. If that's being held onto for up to a year, it's actually difficult to grasp and comprehend how much communication is caught by that. It's an important point.

Rhonda Kirkland: Okay. Thank you.

[*Translation*]

The Chair: Thank you. I'm sorry but your time is up.

Mr. Housefather for five minutes.

[*English*]

Frank Caputo: May I raise a point of order at this point, please, Mr. Chair?

The Chair: Go ahead, Mr. Caputo.

Frank Caputo: I didn't know when the rounds were going to be cut off, so I said I would do it when Ms. Kirkland was done. If Mr. Housefather wants his time afterwards, go ahead.

We have not yet received a ruling from the chair on Mr. Lloyd's point of privilege. I know that you did circulate an email, which was not from the chair, so we haven't had that yet. Given what we are dealing with now.... Somebody has contacted my office and said their brief also hasn't been translated. It was submitted eight days ago if we take them at their word, which I'm obviously prepared to do, and Mr. Lloyd raised a point of privilege.

I wonder if, at the end of Mr. Housefather's round, you could please advise us on that point, because we do need a ruling on that. If there is no ruling, I would be prepared to revive that point of privilege and add my voice to it, given what we've heard today.

Thank you.

● (1635)

The Chair: Thank you, MP Caputo.

[*Translation*]

Mr. Housefather for five minutes.

Anthony Housefather (Mount Royal, Lib.): Thank you, Mr. Chair. I will be sharing my time with Mr. Ramsay.

I want to try to find a solution to the problem raised by Mr. Caputo.

Ms. Saad, you submitted your brief in French and English, did you not?

Christiane Saad: Yes, that's correct.

Anthony Housefather: Okay.

Mr. Chair, I would like unanimous consent for the brief from the Canadian Bar Association and all the other briefs that were sent in both official languages, even if they aren't perfect and were not revised by translators, to be sent to the committee.

The Chair: Indeed, this decision requires the unanimous consent of the committee. The rules we passed at the start of the session are very clear. That said, this kind of motion is possible. Let's quickly check whether there is unanimous consent for this.

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Thank you, Mr. Chair.

I admit that I'm afraid this request will set a precedent, but I understand what Mr. Housefather is trying to do.

Since the brief has already been sent in both official languages, you could forward it to each member of the committee so that we can review it individually.

However, I would not want to set a precedent by accepting a version that hasn't been certified by the translation bureau. If the idea is to send an email to everyone who submitted a brief to explain that the briefs have not been translated and that they should send us a version in both official languages to distribute to committee members, you will understand that I cannot accept that, because it would truly set a significant precedent. Furthermore, I wouldn't be able to assess whether the copy I have in front of me has been translated correctly. If everyone here were English-speaking, it would be easy, because we could have the documents in a single language.

I know what Mr. Housefather is trying to do. In the case of the Canadian Bar Association, I am less concerned that the copy might be of poor quality. As I often tell witnesses, given the limitations of the translation services—which are, in my view, completely unacceptable—we sometimes have to work with highly credible witnesses to have them send us their briefs in both official languages.

Mr. Housefather, I hope you understand that I cannot grant your request, as it would set a precedent that I would prefer to avoid.

The Chair: All right.

In that case, we could follow the proposal put forward by Mrs. DeBellefeuille, namely that organizations such as the Canadian Bar Association that would like their briefs to be made available more quickly could send them directly to members of Parliament. Their email addresses are easily accessible on the House of Commons website. For their part, members of Parliament can use these briefs as they see fit.

Ideally, briefs should be submitted in both French and English. Of course, we cannot prevent an organization from sending a brief to a member of Parliament in only one of the two official languages, but it would be preferable for it to be in both languages. Members of Parliament, for their part, may act at their discretion.

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Thank you for taking the time to discuss this; it is, after all, a very important issue.

If everyone agrees, could you, in your capacity as committee chair, write to Mr. Lymburner at the translation bureau to tell him that this situation is unacceptable and that, when an important bill such as Bill C-22 is being studied, members of Parliament expect priorities to be managed accordingly? It is not normal for the committee not to have the Canadian Bar Association's brief as part of the study of a bill that deals with lawful access. It makes no sense. That said, could you, as chair, file an official complaint? This situation is unacceptable. We need to speak up instead of just accepting it.

Earlier, I was a little taken aback when you said that we weren't the only ones and that we had to work within the limits we have. Personally, that's not what I want to hear from the chair of this committee. What I want is for the chair to stand up for us and tell the translation bureau that the committee is willing to do its job, but that we aren't being given the tools we need to do so. What I expect from the chair of this committee is not for him to give up, but rather for him to fight to secure these services.

The Chair: The chair will do both, Mrs. DeBellefeuille.

First, he will indeed convey the viewpoint you have just so clearly described and, in doing so, defend the committee's interests.

Second, the chair will provide clarification. A few minutes ago, I received more detailed information regarding the Canadian Bar Association's brief. This brief was reportedly submitted in its entirety on May 29. The number of pages it contained exceeded the number that had been communicated two weeks earlier. The final version, containing the correct number of pages, arrived on June 1. It is therefore understandable that, even with considerable resources, it's difficult to meet the committee's expectations and needs. This is in no way a criticism or reproach directed at anyone. It's a learning experience that is also important to understand in the context of the relationship between the committee and the House of Commons.

That being said, I will be more than happy to do as you have requested, Mrs. DeBellefeuille, and we will see how things proceed.

I now turn back to you, Mr. Housefather. You may finish your remarks. You were originally allotted five minutes.

● (1640)

Anthony Housefather: Thank you, Mr. Chair. I think I've probably used up the full five minutes. I'll give the remainder of my speaking time to Mr. Ramsay.

I fully understand Mrs. DeBellefeuille's position. That said, it's really important that we conduct clause-by-clause consideration of the bill. If someone has submitted a brief in both official languages, it shouldn't take that long to determine, just by looking at it, whether the translation is of sufficient quality or not. That's not the same as translating the entire brief. I certainly hope we can at least find a way.

[*English*]

For those who didn't hear that in English, if you have your brief and you want us to see it before, send it to us directly by email. It's firstname.lastname@parl.gc.ca. At least we'll have the choice to read it if you send it.

Thanks, Mr. Chair.

Jacques Ramsay: Mr. Surgenor, I want to come back to something you said.

I would attribute it to your age. You look like a bright fellow, but it was quite naive. If you want to say that the challenges of law enforcement are the same today as they were a long time ago, when officers only had to look into the white pages to find information they needed, that is no longer the case. Police force chiefs from all over Canada spoke with one voice to say that they really needed a lawful access regime.

[*Translation*]

Ms. Saad, if I may, I'll speak to you in French.

You said that the resources were already available to police officers. You're right, but you may not have read the title of part 1 of the bill: It refers to timely access. That's what the police are telling us. Their investigations are stalling or not moving forward because they don't have enough time to access the information. There are too many barriers.

[*English*]

Timely access is what this bill is all about.

[*Translation*]

Mr. Hatfield, you said the government was installing microphones or spyware throughout people's homes. That's not the case, sir, based on the warning Mr. Baber mentioned. You know, the government needs a court order to obtain that information. We ask companies to retain information that isn't accessible to the government unless certain conditions are met and there's reason to believe that this information would lead to a conclusion resulting in a conviction. That's no small matter, Mr. Hatfield.

That's all I'm going to say because I think I've run out of time.

The Chair: That is correct. Unfortunately, your flight of oratory must now come to an end.

Before we suspend the meeting, I would like to tell you that, on the point of privilege, I have contacted representatives from the three different parties and shared with them the observations I have gathered over the past few weeks. I find that there has been no violation of members' privilege, given the usual circumstances we have observed.

This brings me to thank you, distinguished witnesses, for your appearance. I wish you a good day.

For everyone else, we will suspend the session for a few moments.

● (1640)

_____(Pause)_____

● (1650)

The Chair: Good afternoon again, everyone. We're ready to begin the second hour of our meeting.

I'll start by introducing the witnesses.

First, we have Mr. Khaled Alqazzaz from the Canadian Muslim Public Affairs Council, who is joining us by video conference.

Next, we have Mr. Tim McSorley, senior fellow at the Centre for Free Expression. He is here in person.

We also have Mr. Udbhav Tiwari from Signal, who is joining us by video conference.

I welcome to our distinguished witnesses and thank you for joining us.

Let's now move on to the presentations. You will each have five minutes to speak. Let's begin with Khaled Alqazzaz.

You have the floor, Mr. Alqazzaz.

[*English*]

Khaled Alqazzaz (Executive Director, Canadian Muslim Public Affairs Council): Thank you, Mr. Chair.

Assalamu alykum. Peace be with you. Thank you for the opportunity to appear today.

My name is Khaled Alqazzaz, and I am the executive director of the Canadian Muslim Public Affairs Council. CMPAC is a not-for-profit organization dedicated to advancing civil liberties, addressing systemic Islamophobia and ensuring that Muslim perspectives are represented in public policy.

CMPAC submits that Bill C-22 should be withdrawn. At a minimum, part 2 of the legislation, the supporting authorized access to information act, should be removed in its entirety, and the provisions in part 1 that lower the threshold for access to subscriber information should be amended.

For Muslim Canadians, surveillance powers carry a particular significance. Muslim communities have been disproportionately affected by national security and counterterrorism measures, particularly where expansive investigative authorities have operated with limited accountability and oversight. These experiences reinforce concerns that expanded surveillance powers disproportionately affect racialized and religious minority groups.

Privacy scholars and legal experts—in a joint letter sent to the Prime Minister by civil liberties organizations, refugee rights organizations, academics and digital rights organizations—concluded that, if adopted as is, “Bill C-22 will be the most expansive invasion of Canadian privacy rights in modern history, and will put the cybersecurity of everyone in Canada at unacceptable risk”.

The details of our submission will be shared with the committee right after this meeting. However, here is a summary of our main concerns.

Of particular concern is the creation of new production orders for subscriber information based on the lower standard of “reasonable grounds to suspect” versus “grounds to believe”.

Part 2 of the bill raises even greater difficulties. The SAAIA grants broad regulatory and ministerial powers to compel service providers to facilitate access to information and retain metadata. The practical effect would be to increase the state's ability to collect, organize and analyze information capable of revealing religious participation, political engagement, community relationships and patterns of association. When metadata is collected and retained on a broad scale, such information permits forms of associational surveillance capable of exposing lawful religious, charitable and advocacy activities.

The second part with regard to part 2 is that by authorizing the government to require all electronic service providers to modify their systems and develop technical capabilities that facilitate access to information, Bill C-22 risks creating vulnerabilities that could weaken the security of Canadians’ communications and personal information. Once vulnerabilities exist, they may be exploited not only by Canadian authorities but also by foreign governments, cybercriminals and other malicious actors.

Also, in part 2, the extensive reliance on secret orders is quite problematic. Powers exercised through confidential directives with limited transparency create obvious accountability deficits. Fundamental rights require meaningful oversight and transparency.

Now I'll leave you with two examples, one from our community.

Many members of the Muslim community across Canada are immigrants, refugees and individuals with family connections in countries characterized by weak rule of law, political instability or authoritarian governance. In such contexts, the low threshold of “reasonable grounds to suspect” for foreign entities to request personal data held in Canada, along with the lack of dual criminality provisions in changes to the Mutual Legal Assistance in Criminal Matters Act, can create serious risks, including transnational repression, intimidation of family members, travel restrictions or other forms of retaliation. These concerns are particularly significant where information may be requested or shared based on conduct that is not necessarily unlawful under Canadian law.

The second example is about concerns that extend beyond any single community and that could affect all Canadians, including members of Parliament who engage in international travel or diplomatic activities. Several MPs have already been investigated for potential foreign interference. By lowering the threshold to “reasonable grounds to suspect,” Bill C-22 would permit the collection of significant amounts of personal information. Such collection may impact suspected MPs and a broader circle of friends and family. This data can potentially be requested by foreign state agencies as part of an investigation, having direct and indirect impacts on the individuals investigated. While such measures may be justified in limited cases, their impact often extends beyond the individual under investigation.

● (1655)

Furthermore, as a result of the legislation, ESPs would face additional vulnerabilities, exposing them to higher risks of hacking and data breaches, impacting every citizen, activist and, potentially, senior politician and subjecting them to extortion and targeting.

To wrap up, expanded surveillance powers could disproportionately affect Muslim, racialized, indigenous and other marginalized communities. For this reason, CMPAC urges the withdrawal of Bill C-22 for review. Public safety is a legitimate objective, but measures pursued in its name must remain consistent with constitutional rights, fundamental freedoms and democratic accountability.

Thank you.

[*Translation*]

The Chair: Thank you very much, Mr. Alqazzaz.

Mr. McSorley, you have the floor for five minutes.

Tim McSorley (Senior Fellow, Centre for Free Expression): Thank you, Mr. Chair.

[*English*]

On behalf of the Centre for Free Expression, I want to thank all of you for the opportunity to appear here today before you.

Bill C-22 poses a serious and unacceptable risk to the privacy right of Canadians—both as an individual right and a social right essential to participate meaningfully in democratic discourse. The Centre for Free Expression's work is premised on understanding that democracy is a regime founded on ongoing public discourse about what is legitimate and what is illegitimate in society—a discourse that is necessarily without any guarantor and without any end, and one we all have a right to participate in and to be informed by.

Privacy is fundamental for freedom of expression and democratic discourse, specifically what Neil Richards has termed “intellectual privacy”, which is the “protection from surveillance or interference when we are engaged in the process of generating ideas—thinking, reading,” and when we are discussing these with those close to us “before our ideas are ready for public consumption.” In our evolving digital world, much of our reading, thinking and private communications are mediated by electronic technologies that make possible unprecedented forms of surveillance by the state, digital platforms, marketers and even those in our social networks.

The right to privacy is recognized as a human right in international law that Canada has signed and ratified. It is enshrined in the United Nations' 1948 Universal Declaration of Human Rights, which Canada supported and endorsed. While Canada's Charter of Rights and Freedoms does not mention privacy specifically, our courts have made clear that section 8 protects privacy.

In R v. Spencer, Justice Cromwell wrote, for a unanimous Supreme Court, in paragraph 15, the following:

> This Court has long emphasized the need for a purposive approach to s. 8 that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society....

Further, at paragraph 36, he wrote:

> The nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. The analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought.

Finally, at paragraph 41, he wrote:

> There is also a third conception of informational privacy...the understanding of privacy as anonymity. In my view, the concept of privacy potentially protected by s. 8 must include this understanding of privacy.

In R v. Marakah, Chief Justice McLachlin discussed the privacy implications of modern electronic communications. She wrote:

> Preservation of a “zone of privacy” in which personal information is safe from state intrusion is the very purpose of s. 8 of the Charter [and] this zone of privacy extends beyond one's own mobile device; it can include the electronic conversations in which one shares private information with others. It is reasonable to expect these private interactions—and not just the contents of a particular cell phone at a particular point in time—to remain private.

Bill C-22 is the latest in a long string of proposals to undermine Canadians' right to privacy in the name of fighting crime and protecting national security. While all rights are weighed by our courts in light of these competing interests and priorities, the proponents of Bill C-22 have lost sight of the priority that our charter and courts have given to protecting expressive freedom, and hence to the privacy rights that help make political expression and democratic discourse possible.

Bill C-22 would also supercharge state surveillance by, first, establishing a new low threshold for production orders under the Mutual Legal Assistance in Criminal Matters Act, so foreign entities could submit a request to the Minister of Justice for the production of transmission data or subscriber data in the possession or control of a person in Canada. To be granted, the request would only have to meet the low bar of “reasonable grounds to suspect”. There would be no dual criminality requirement, meaning the foreign offence need not also be an offence in Canada.

Second, it would create the framework for Canada to ratify the second additional protocol of the Budapest convention, a multilateral data-sharing treaty that attempts to expedite the speed and volume of data sharing among foreign law enforcement agencies at the expense of human rights.

Third, it would make possible a Canada-U.S. cross-border data-sharing agreement, which Canada is currently negotiating with the United States under the U.S. CLOUD Act. As the Citizen Lab's Kate Robertson wrote that this would mean “US surveillance activities covered by the agreement would no longer require oversight from Canadian authorities or judges, thus relinquishing a core element of Canada's sovereignty under international law.”

● (1700)

Finally, the supporting authorized access to information act, through both public regulations and secret orders, would allow the government to require the broadly defined category of “electronic service providers” to make wide-ranging and drastic modifications to their systems in order to facilitate access for law enforcement, threatening encryption. It will also require all ESPs to retain sensitive personal data about users for up to a year, without adequate safeguards to protect against security vulnerabilities that such orders will create. The new regime would also lack adequate accountability or transparency provisions.

Thank you, and I look forward to your questions.

[*Translation*]

The Chair: Thank you very much for those opening remarks.

I now give the floor to Mr. Tiwari, who is onscreen, for five minutes.

[*English*]

Udbhav Tiwari (Vice-President, Strategy and Global Affairs, Signal): Thank you, Chairperson and members of the committee.

I am Udbhav Tiwari, vice-president of strategy and global affairs at Signal.

Signal is a non-profit. We make the world's most widely used, truly private messaging app, and the encryption protocol we built, the Signal protocol, is the gold standard that much of the industry beyond us relies on. It is essential for providing the core infrastructure for the fundamental human right to privacy.

Those who depend on us and on this technology are regularly subjected to surveillance around the world. However, it is vital for us to recognize that it is because of how we operate, at the frontier of global cybersecurity, that we understand intimately how technical architecture protects human safety and how easily badly drafted laws can dismantle these critical protections.

In its current form, Bill C-22 would convert the everyday tools Canadians rely on into a sprawling, insecure surveillance apparatus. To be up front, Signal will not build infrastructure into our service, and we will also not build surveillance into our service. If we are ever forced to choose between betraying the people who rely on us and leaving a market, we will leave.

One fact shapes everything I will say: Signal collects almost no data about our users, by design. It is this property that leads us to enjoy the reputation we have, including among Canadians. Bill C-22 could force us to rewrite our code, dismantle our robust privacy architectures and design surveillance into our systems. Let me give you three concrete pictures of how chilling such a proposition is.

First is undermining encryption. Bill C-22 creates an open-ended power to compel a company to re-engineer its own service to enable government access. We have seen where this leads. We know it is never one device. Once you build a mechanism to break your own protections, that mechanism exists, and it can be identified and exploited by anyone with the time and resources to do so. As security experts have warned for over 30 years, there is no back door that only the good guys can walk through.

Second is deliberately engineering weaknesses. This is the provision that should alarm anyone who relies on the safety of private messaging and on technical services more broadly. The powers in this bill are broad enough to compel a service like Signal to sell out our users, to do things like silently create hidden accounts and slip them into private group conversations, to manufacture a participant the other members cannot see, and to do the same to other apps, services and infrastructure.

Third is forced metadata retention. As we've established, we built Signal to retain as close to no data as possible. This includes intimate metadata. Bill C-22 would let the government compel us to construct the very surveillance apparatus we have refused to build, in order to log who is talking to whom, when and from where, for up to a year. Do not let the word “metadata” reassure you. Metadata is the 2 a.m. phone call, the clinic you contacted, the lawyer you retained, the organizer you met and the journalist you trusted. In aggregate, it reveals as much, if not more, about individuals as content—often more. A mandate to retain it would build a goldmine of intimate data where none exists today, sitting ready for any foreign adversary or criminal who breaches it. Mathematics does not care about executive intent. A back door built for the good guys is simply a vulnerability waiting for the bad guys to find.

None of this is hypothetical. Australia passed a similar regime in 2018, which required over 150 amendments before it could pass, and Australia's own Parliamentary Joint Committee on Human Rights found it incompatible with the rights to privacy and free expression. Under it, the definition of a “covered provider” stretched to fast food chains and shopping mall Wi-Fi. We've seen similar things play out with Apple and iCloud in the United Kingdom, and the Salt Typhoon hack in the United States as well, both of which have been covered in great detail by others testifying before this committee.

Let me end with what genuine reform of the law would require. To update this bill for the technical realities of our current era, part 2 of C-22 should be withdrawn. Its core defects cannot be repaired with targeted amendments.

● (1705)

If withdrawal is not politically feasible, as much as it is the right course of action, then the following safeguards should be considered non-negotiable for any amendments that improve these provisions.

The first is prior judicial authorization. Any order to alter a security system must be approved in advance by a court and not imposed—

The Chair: I'm sorry, Mr. Tiwari. You'll need to speed up another 10 seconds. There will very likely be an opportunity for you to continue with MPs. I'm sorry to do that.

Let me turn the floor to MP Caputo for six minutes, please.

Frank Caputo: Thank you, Mr. Chair.

You can use my time to finish up your opening statement, sir. Go ahead.

Udbhav Tiwari: Thank you. I'll be very quick.

Second is independent technical scrutiny. There must be expert independent assessments of feasibility and security before any obligations or orders under part 2 take effect.

Third, and finally, is a hard line on encryption and metadata. The law must prohibit degrading or bypassing encryption and prohibit forcing any provider to collect metadata that it does not already hold.

To repeat, Signal will not build surveillance into our service. If we are ever forced to choose between betraying the people who rely on us or leaving a market, we will leave, but Canada should not force anyone to make this choice. You cannot make Canadians safer by breaking the tools they rely on for protection from hackers, hostile nations and everyday transnational surveillance.

Thank you for your time. I look forward to your questions.

● (1710)

Frank Caputo: Thank you very much.

One question I have is this. The government has called this bill “encryption-neutral”, whatever that means. I have no idea what that means. I think it's a little bit of a cute phrase to try to avoid the question. The minister himself has said that they will deal with encryption.

Is it even possible to have any amendment that might satisfy you, given how this process has gone? I'm sure you've been observing it. I'm sure you've seen the rushed nature of this process. The fact of the matter is that we probably need more time on this bill. It's not that we haven't spent substantial time. It's that we've crammed so many witnesses into a short period of time that I don't really feel that we heard adequately from witnesses.

Number one, would you agree with all of that? Number two, is there anything that could possibly satisfy you with respect to part 2 on your encryption concerns?

Udbhav Tiwari: Yes, I absolutely agree that the way part 2 is currently drafted is incompatible with the fundamental human right to privacy. It is why our primary recommendation is that it be scrapped entirely.

If it is not feasible to do so, we think that certain targeted changes should be the absolute foundation for any legislation that looks like part 2. Even those will not address all of our concerns and will in fact continue to leave various executive actions that could harm the privacy and security of everyday Canadians.

Frank Caputo: Thank you.

For the other two witnesses, I did mention my view that this bill has been quite rushed. I'm not sure if either of you or all three of you were watching earlier, but we've just found out that briefs that were submitted in some cases over a week ago did not make it to committee, and amendments were due yesterday. It's really begging the question of, if we had an amendment or a proposed amendment, whether we could even debate it.

I'm just getting a sense from all of you, given all of that, whether this bill feels rushed.

I'll start with you, Mr. McSorley. Then we'll go to the two on video, please.

Tim McSorley: Thank you.

Yes, we agree that this process has felt rushed both in the number of days of study and the amount of time that the study has taken.

As well as being a senior fellow with the Centre for Free Expression, I'm also national coordinator with a coalition called the International Civil Liberties Monitoring Group. We submitted a brief in English to the committee on Sunday, May 24. We've been told that it will be circulated—hopefully—on Friday.

We understand that it's later in the process and there is a strain on resources, so this isn't a criticism of the hard work that the staff are doing, but the speed at which the study has been progressing. From our experience—and I've been with ICLMG and doing this for 10 years—it's incredibly difficult to get a brief in on time for it to be translated in the amount of time that this study has been progressing. It has been much too short.

We have significant concerns and we have colleagues from other organizations whom we believe should be here today. The Citizen Lab and the Canadian Civil Liberties Association came out with an incredible 55-page analysis of this bill, yet it likely is much too late in the process and has come out after amendments were due. This is a grave concern of ours.

Frank Caputo: Do either of you gentlemen on video have anything to add, in 30 seconds, please?

Khaled Alqazzaz: Thank you, MP Caputo.

Briefly, we actually looked into the amount of consultation, as one of our recommendations, and we do not feel that there was enough evidence put forward to demonstrate that there is a need for additional legislation or to go into this much detail. That's one point.

The second point is that we're making this contribution to note the impact on marginalized groups and racialized communities. We feel that even in that space, very little impact analysis or engagement was actually done on or with these different communities. As marginalized or vulnerable communities, we see or feel the impact much higher than others—

Frank Caputo: I'm sorry. I have to interrupt you there, sir. I do have to give notice of motion.

I'm giving notice of the following motion:

> That, in relation to the ongoing study of Bill C-22, an Act respecting lawful access:
>
> a) the study be extended to accommodate further examination of Part 2 of the bill which would enact the Supporting Authorized Access to Information Act, provided that the following witnesses appear separately, for at least one hour each:
>
> i. the Minister of Industry, in relation to the impact on electronic service providers and their industry;
>
> ii. the Minister responsible for Canada-U.S. Trade, in relation to trade and security implications raised by American lawmakers;
>
> iii. the Secretary of State (Combatting Crime);
>
> iv. the Privacy Commissioner;
>
> b) the committee receive an additional eight hours of witness testimony, provided that the committee prioritize hearing the testimony of representatives from NordVPN, ProtonVPN, ExpressVPN, Windscribe, DuckDuckGO, Migrant Workers Alliance for Change, British Columbia Civil Liberties Association, Canadian Anti-Monopoly Project, Canadian Council for Refugees, Migrant Justice Clinic, International Civil Liberties Monitoring Group, Ontario Council of Agencies Serving Immigrants, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, and the testimony of Glenn Greenwald, Safiyya Ahmad, Noura Aljizawi, Brent Arnold, Teresa Scassa, Jane Bailey, Colin Bennett, Ron Deibert, Lex Gill, Pantea Jafari, Michael Karanicolas, Shera Kelly, Kate Robertson, and Maria Vamvalis, in addition to additional testimony deemed relevant by the committee;
>
> c) the Chair be authorized to seek additional meeting time to accommodate this testimony in a timely manner;
>
> d) the Chair only be authorized to schedule a meeting for the purposes of clause-by-clause consideration of Part 2 of the bill after the witnesses listed in part a) have appeared, and the number of hours of testimony in part b) have been received.

That is my motion. Thank you.

● (1715)

The Chair: Thank you, MP Caputo, for this notice of motion.

Let me now turn to MP Powlowski for six minutes, please.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Mr. McSorley, you talked about the right to privacy and wanting to be able to read whatever you'd like before forming your opinion on something. My understanding of this law is that it specifically excludes access to content and information on a person's web browsing history and social media activity. I understand it would allow the government to access IP addresses, for example.

Could you lead me down your sequence of thinking as to how this violates your right to privacy? Can you give me concrete examples of how IP addresses and phone numbers are going to violate your right to privacy?

Tim McSorley: Thank you for the question. I think it is very important.

It's true that I mentioned what we read, but it's also who we communicate with and how we discuss things. It's about our private lives. Looking at Bill C-22, I think the issue goes much further than IP addresses and names. For example, the production order for subscriber information includes what kinds of services you were able to access from the service provider, when you accessed them and where you accessed them from. That goes much further than just an IP address and is revealing of an individual's—

Marcus Powlowski: Can you tell me about what you said on the kinds of services provided? I don't know. I'm a bit of a simpleton. When I go to browse the web, I just access a website. I read the information. I maybe text people.

What other kinds of access are you talking about?

Tim McSorley: The production orders under part 1 aren't limited to just telecommunications or electronic service providers. The wording of the law is that it's to any entity that provides a service within Canada. That isn't just browsing a website. I'll specify here. The confirmation of service demands have an explicit exclusion for medical information and for privileged information. That exclusion does not apply to the production orders.

For example, if I access an online portal to make appointments with my doctor or to access certain services, even what services they hold on file for me, that would be available through these new production orders. It is highly revealing. It goes much further than simple IP addresses and whether or not I went to a certain website.

That's just the production orders in part 1. That's not to mention what kind of information could be highly revealing in terms of the metadata that's collected under part 2. I realize that for law enforcement to access that, they would have to have lawful authorization, but having the scope of information there.... We have to be realistic.

Looking back over the last 10 years, every time we see the ability for police, CSIS or intelligence agencies to access more information, they do that. For example, with CSIS's dataset collections, they were able, under Bill C-59, to begin collecting datasets about Canadian individuals in publicly available information. The NSIRA found that shortly after getting those powers, they went further than they were allowed. Under this, they would have the lawful authorization to use that to also request and access datasets of metadata held by electronic service providers.

It's an incredibly complex law. I understand your point that there are certain things we do online that are not necessarily revealing, even though the Supreme Court has agreed that IP addresses should be protected under privacy laws, but that is a tiny part of what Bill C-22 is proposing. The fact that this information could be acquired has a direct impact on privacy and on our ability to engage in free expression.

● (1720)

Marcus Powlowski: Is part of the concern.... I gather that one of the things this law would allow would be for the government to access whom I was talking with on the phone. I don't know how many colleagues' phone numbers they have on their phones. I have, I think, a thousand on mine. I'm pretty sure some of them have, at some point or another, engaged in criminal activity. I'm sure the Conservatives have even more on their phones.

Voices: Oh, oh!

Marcus Powlowski: Is the concern that the government could access this, find someone's number whom it suspects of engaging in criminal activity, and that would be sufficient for it to get the further judicial order to start looking at the content of the information?

Tim McSorley: The concern is of the association of the data that could be made. That's one part of it. As I mentioned for datasets, it's also this idea of collecting and using this kind of information in order to then try to engage in predicting criminality or predicting threat assessments. The ability to do that has not been proven. In fact, as we know, there are concerns around biases in those kinds of algorithms and that kind of analysis.

We've seen in the past, under national security investigations, that this idea of guilt by association is enough to engage in very harmful investigations.

Marcus Powlowski: You're worried that the metadata, if I may have contacted three people in the last year who are involved with some sort of criminal activity, would then put me on some sort of watch list, and I would be subject to heightened surveillance by the government because of that.

Tim McSorley: That would be part of our concerns, yes.

Marcus Powlowski: Could I ask Mr. Alqazzaz the same question?

I'm certainly involved with helping Afghan interpreters come to Canada. I've had various conversations with people in Afghanistan. I would certainly share their concerns that if the IP addresses of people in Afghanistan put me at risk and put me on some sort of heightened security, it would be pretty hard to escape that if you're talking to anyone in Afghanistan at the current time. Is that a concern of yours?

Khaled Alqazzaz: Thank you for this question.

It's important that I share with you the opposite perspective, basically.

Canada has hosted so many refugees from Afghanistan and many activists in different forms, in exile from Africa, from Iran and from many different countries. They are actually under extreme pressure and surveillance by foreign state agencies. Unfortunately, for some of them, this bill will enable more access to this information through requests from foreign states, even if they are not subject to fault under Canadian law.

We've seen incidents where activists in exile here in Canada were targeted by their regimes. There was an assassination of an Indian activist—

The Chair: I'm sorry to interrupt. I was distracted. I should have stopped Mr. Powlowski a few seconds ago.

[*Translation*]

Mrs. DeBellefeuille for six minutes.

Claude DeBellefeuille: Thank you very much, Mr. Chair.

I want to speak to you, Mr. Tiwari. I think you must have guessed as much.

Since the government holds a majority and is truly committed to passing Bill C-22, we are convinced that the bill will be passed by any means the government can use to achieve this. It must be said that the minister is very open to amendments. In that regard, we have even introduced amendments to clarify all issues related to encryption and metadata retention. In fact, when I say “we”, I mean myself, on behalf of my party. We have proposed a series of amendments that we hope will provide some assurance that privacy is properly respected and that there is no infringement of privacy.

Based on your testimony, you do not believe that certain amendments could provide you with any such assurance. Have I got that right?

● (1725)

[*English*]

Udbhav Tiwari: Yes. I did say so, specifically with regard to the provisions in the law that allow the government to order platforms to deliberately make changes to their services.

For example, if an order were to be passed that Signal should start collecting data that it does not collect today, or that Signal should create a feature that allows law enforcement to silently join groups and observe conversations, both examples are of things that do not directly touch encryption but that negate the very purpose of encryption. We believe that any law that contains such technical access measures is incompatible with privacy.

[*Translation*]

Claude DeBellefeuille: Perhaps my question wasn't clear.

I find you to be a highly credible witness. I'm not saying that the other witnesses aren't credible, but I know the reputation of your organization. Your strength is protecting your clients and their security.

What would it take to protect the Signal organization? What do you think needs to be done to properly ensure privacy protection and, above all, to reassure you so that you can stay here and not leave Canada? What kind of assurance would you need?

[*English*]

Udbhav Tiwari: At the risk of repeating myself, I will say that we believe it is very challenging to see how proposed part 2 could be amended in a way that would not pose a serious threat to Signal.

If it is politically unfeasible for proposed part 2 to be removed, then we would request two crucial changes. The first is that an explicit amendment be introduced that does not allow the government to weaken encryption in any product, either directly under the provisions of the law or via indirect provisions, such as technical capability notices or production orders.

The second—

[*Translation*]

Claude DeBellefeuille: I just want to clarify something, Mr. Tiwari. You're telling us that, if the government goes ahead despite all the testimony heard about the dangers of part 2, some key amendments will be needed, and you're in the process of listing them.

Time is of the essence, since we'll be starting clause-by-clause consideration of the bill on Thursday. I was wondering whether you had your amendments on hand and whether you could pass them on to us quickly so that we can take a look at them. If so, I'll let you explain them to us.

What amendments to part 2 could you explain to us verbally while we're waiting to see them?

[*English*]

Udbhav Tiwari: We would be very happy to share with the committee specific language with regard to the amendments in proposed part 2. At a high level, those changes will pertain to, number one, explicitly protecting encryption; number two, making sure that metadata collection cannot be expanded to compel the collection of metadata, but must be limited to metadata the provider already collects; and three, regarding mandatory judicial authorization of these orders under proposed part 2, making it not just an executive action but one overseen by an independent judicial authority.

[*Translation*]

Claude DeBellefeuille: Thank you.

Mr. McSorley, we recently learned that the Canadian Security Intelligence Service has broken the law on a number of occasions. It failed to comply with the Canadian Charter of Rights and Freedoms and other current legislation. You're probably aware of this, since protecting privacy is your main mission.

Are you concerned about the fact that the Canadian Security Intelligence Service is currently breaking the law and that, basically, the bill will give it even a bit more power? Are you worried about this?

● (1730)

Tim McSorley: We're indeed aware of the report from the National Security and Intelligence Review Agency. It's quite worrying.

[*English*]

We're definitely concerned. Time and again.... This is not the first time that CSIS has been found to be either engaging in unlawful activity or pushing the boundaries of what they're allowed to do. We saw this with Bill C-70, the foreign interference act. We saw this with the National Security Act, and now we're seeing it again with this act. Every time we hear this is happening, they're rewarded with new powers, and there's very little—at least no public—discussion of what the repercussions are for the individuals and for the service when they do....

It's frustrating to see that we only learn about this because of an access to information request, and that it's not the kind of information that NSIRA and others are able to share publicly so we can have these public debates. If there wasn't this access to information request, we would have never known of the 20 instances, approximately, within one year of CSIS engaging in unlawful activity.

[*Translation*]

Claude DeBellefeuille: Thank you.

[*English*]

The Chair: Thank you very much.

Let me turn to Ms. Kirkland for five minutes, please.

Rhonda Kirkland: Thank you, Chair.

Mr. Tiwari, I have two brief questions for you, and you should probably be brief in response.

Is it fair to say that Signal's position, which you've laid out very clearly today, is not about resisting lawful access generally?

Udbhav Tiwari: No. Signal's position is that laws should not compel service providers to start collecting information that they do not already collect.

Rhonda Kirkland: Thank you.

When Signal says it would exit Canada rather than comply, is that a decision triggered only by direct access to messages, or would metadata retention and system redesign requirements alone be enough to make compliance impossible?

Udbhav Tiwari: The last two examples that you just stated would also be enough to make us not serve the market, as they would fundamentally change our product.

Rhonda Kirkland: Thank you.

With Bill C-22, we're not talking about a minor amendment. It goes to the core of how Canadians' privacy is protected, how their digital communications may be accessed and how confidence in our institutions is either strengthened or weakened for years to come.

We as Conservatives are committed to seeing part 1 potentially become law before the summer adjournment, but part 2 raises some serious concerns for us—and for all of us, it should—as we've listened at this committee over several sessions.

There's major government overreach and significant expansion of government authority, and I truly believe that this bill needs further study if the committee is going to fix this flawed Liberal surveillance law. When legislation touches Canadians' private communications and personal data, our responsibility is to slow down, to examine it carefully and to fully understand the consequences before proceeding.

We have also heard a CSIS official acknowledge that no technical system is 100% secure. Lawful access mechanisms could be exploited. At the same time, the Public Safety minister acknowledged that trust is undermined when Canadians do not understand how their information is used. That goes to the heart of this issue, so we have to ensure that every risk is examined and every safeguard tested. That requires time, scrutiny and care.

Canadians don't want us to rush. They're asking us to get it right. We shouldn't be racing.

Accordingly, I'd like to give verbal notice of the following motion:

> That the committee report the following recommendation to the House:
>
> That the House grant the Standing Committee on Public Safety and National Security the power to divide Bill C-22, an Act respecting lawful access, into two parts provided that:
>
> a) Bill C-22A consist of clauses 2 to 40, which would amend various Acts to modernize certain provisions respecting the timely gathering and production of data and information during an investigation, including amendments to the Criminal Code, the Foreign Publishers Advertising Services Act, the Mutual Legal Assistance in Criminal Matters Act, the Canadian Security Intelligence Service Act, the Controlled Drugs and Substances Act and the Cannabis Act;
>
> b) Bill C-22B consist of clauses 41 to 47, enacting the Supporting Authorized Access to Information Act which establishes a framework for ensuring that electronic service providers can facilitate the exercise, by authorized persons, of authorities to access information conferred under the Criminal Code or the Canadian Security Intelligence Service Act, as well as consequential and related amendments to the Intelligence Commissioner Act;
>
> and that both bills contain provisions that will subject them to a parliamentary review, such as those contained in clause 48.

Thank you, Mr. Chair.

● (1735)

The Chair: Thank you for that notice of motion, Ms. Kirkland.

The time is up, MP Caputo, unless it's a point of order.

Frank Caputo: Mr. Chair, thank you very much.

The Chair: Is it a point of order?

Frank Caputo: This is on privilege, and I would like to move the following privilege motion that, given that (a) the Privacy Commissioner provided documentation to the committee in relation to the study of Bill C-22 but that documentation was not distributed to the committee in a timely manner, preventing members from preparing for his appearance and incorporating his recommendations into amendments prior to the original deadline; (b) OpenMedia provided documentation to the committee, but it was not distributed in a timely manner, preventing members from preparing their testimony; and (c) Apple provided a brief to the committee over one week ago, but that documentation has not been provided to the committee ahead of the deadline for amendments; it be resolved that, in the opinion of the committee, the members' privileges have been breached; that the clerk be instructed to compile the relevant facts and evidence; and that those facts and evidence be reported to the House.

Mr. Chair, I don't think anybody likes to move a privilege motion, but—

Anthony Housefather: I have a point of order.

The Chair: MP Housefather, go ahead.

Anthony Housefather: Mr. Chair, you previously ruled today that this wasn't privilege. You actually ruled on this point, which is the subject of this motion. A motion cannot be moved on a point of privilege, and it cannot be moved, particularly, since you already ruled on this, Mr. Chair.

The Chair: I'll give a few more seconds to MP Caputo, but....

Frank Caputo: With all due respect, that was actually with respect to Mr. Lloyd's point of privilege. We have now learned—

The Chair: This is—

Frank Caputo: I have the floor here, please. We have now learned that—

An hon. member: No, you don't.

The Chair: No, this is a point of privilege.

Frank Caputo: Yes.

The Chair: The motion that you're moving, what you call a motion of privilege, as MP Housefather has already said, I already ruled on that point earlier.

Frank Caputo: Well, no, this a different point of privilege—

The Chair: If there is something else that you would like to point—

Frank Caputo: Yes, there is something else I would like to point out: Amendments were due yesterday. That wasn't the case with Mr. Lloyd's point of privilege. We found out that three witnesses who came here today—

The Chair: I'm sorry, MP Caputo, I know you have things to say, but we have witnesses to hear.

If it's not related to the matter dealing with business—

Frank Caputo: Privilege takes priority over committee business. It is privilege—

The Chair: I'm sorry. I am the chair, and I'm going to say clearly what I said earlier, which is that I have already ruled on this matter of privilege.

Frank Caputo: You did not rule on my matter of privilege.

The Chair: Is this something new?

Frank Caputo: This is something new because we were asked to put in amendments yesterday—

The Chair: I will suspend for a couple of seconds, and then we'll come back.

● (1735)

_____(Pause)_____

● (1740)

The Chair: I'll say it in English, and I hope everyone will understand my broken legal expertise, both in French and in English.

This is, in my view, not a point of privilege. I've already ruled on that. Now, if the committee wants to question and to overrule my decision, that's the privilege of the members of the committee. However, I've already ruled on this matter of privilege, and I will, therefore, move to the witnesses.

Rhonda Kirkland: I have a point of order, Mr. Chair. I would argue that—

The Chair: Ms. Kirkland, it has to be a point of order.

Rhonda Kirkland: I believe it is a point of order because this is a different subject matter completely.

We have learned—and I don't want to be disappointed here—more information during this meeting, which required a new point of privilege. In the previous meeting, we did not have amendments due in this meeting. This is a different scenario. We learned of more things we have missed, and we haven't received.

I would argue that it is absolutely a different point of privilege. I would completely disagree with your ruling if you were to rule that it wasn't. I think you need to see that this is a new set of information that we have not received. It's totally different from Mr. Lloyd's.

An hon. member: Then challenge the chair.

The Chair: I have Mr. Baber, and then we'll move on.

[*Translation*]

Claude DeBellefeuille: In any case, the interpreter didn't hear any of it, I can tell you that.

The Chair: What did you say, Mrs. DeBellefeuille?

Claude DeBellefeuille: There's obstinacy and it wasn't interpreted.

As you know, Mr. Chair, I think that the interpreters here are the best on the Hill.

The Chair: You're right to say so, because we think so too.

Claude DeBellefeuille: Yet even though they're the best, they understood absolutely nothing of the obstinacy that I just witnessed.

The Chair: Good point. I think that everyone should understand it properly.

[*English*]

Go ahead, Mr. Baber.

Roman Baber: Should she not repeat it then? If it wasn't interpreted, should it not be repeated?

Frank Caputo: I think it should be, but what do you think?

The Chair: Let's see if Mr. Baber has an additional point to make.

Roman Baber: Chair, you have ruled on a different set of facts. What happened at the commencement of this meeting is that Mr. Caputo asked to resurrect a previous question of privilege made by Mr. Lloyd. Since then, we have obtained not just new information but a new set of facts that also gives rise to privilege. This is privilege that you must be compelled to rule on, even if you wish to refer to your previous ruling for guidance.

We have a material change in facts. We have now learned of at least two stakeholders today who have submitted briefs. One is OpenMedia. It submitted a brief two weeks ago.

Marianne Dandurand: I have a point of order.

● (1745)

Roman Baber: Another one is Apple. It submitted a brief eight days ago.

In the meantime, while the House of Commons is receiving criticism, it's the government that is thrusting and pushing clause-by-clause to start the day after tomorrow. Without having access to briefs that can be very instructive in this process, this is a clear violation of privilege. I ask you to rule on this set of facts, please.

The Chair: Go ahead, MP Dandurand.

[*Translation*]

Marianne Dandurand: Mr. Chair, I think that we've already talked about all this. I think we can stop talking about this and get back to the work that we were doing. It's absolutely not a point of privilege. There hasn't been any violation. I think that we can pick up where we left off.

We have witnesses waiting to continue their testimonies. The opposition members wanted to hear from these witnesses. So I think that we should get back to business and continue to speak with these witnesses to hear their ideas, since they think that their ideas are very useful. I would like to be able to ask them questions.

The Chair: Mr. Ramsay, you have the floor.

Jacques Ramsay: Mr. Chair, with all due respect to my colleagues, I would say that the translation issue occurs in all parliamentary committees on the Hill. This issue has been around for a number of years. This isn't an issue for debate today. It isn't a Bill C-22 issue. The opposition is trying to get mileage out of a red herring.

You already voted on the motion, Mr. Chair. I think that we can get back to business. We have important witnesses to hear from and I suggest that we do so.

The Chair: Okay.

I'll say it in French this time. That way, there won't be any problems interpreting from English to French.

You heard my ruling. There isn't any point of privilege this time, just as there wasn't any last time.

If the committee would like to question or challenge my ruling, it's possible to do so.

[*English*]

Frank Caputo: I would like to respond to that point of order.

The Chair: No, MP Caputo, we have—

Frank Caputo: Mr. Chair, so he gets to call—

The Chair: No, MP Caputo, I'm sorry.

I am the chair, and I'm going to—

Frank Caputo: I understand, but he called it fake.

The Chair: We're going to suspend and adjourn soon.

● (1745)

_____(Pause)_____

● (1745)

[*Translation*]

The Chair: I call the meeting back to order.

To wrap up the discussion, I'll ask the clerk to check whether the committee members want to question my ruling on the point of privilege.

[*English*]

Frank Caputo: Is this regarding the point of privilege?

The Chair: No. We are going to end that discussion with a clear decision on whether the committee members want to overrule my decision on the question of privilege I described before the break.

Mr. Clerk, please proceed with a roll call.

[*Translation*]

Claude DeBellefeuille: Mr. Chair, it's that—

[*English*]

The Chair: I am doing it now, and we'll see what the outcome is.

Mr. Clerk, please go ahead.

● (1750)

[*Translation*]

Claude DeBellefeuille: Excuse me, but I don't even know what we're talking about. Is this a motion tabled spontaneously?

The Chair: Yes.

Claude DeBellefeuille: What's the motion, exactly?

The Chair: A question was asked about a point of privilege.

Claude DeBellefeuille: Yes.

The Chair: I informed the committee of my ruling.

Claude DeBellefeuille: Was it about the documents? What was it about?

The Chair: It was felt that a violation of the members' privilege had occurred because of delays in translation. Reports from the Privacy Commissioner were discussed. I informed the committee of my ruling that no violation of the members' privilege had occurred. This ruling was challenged, which is entirely possible. The clerk will check whether the majority of committee members want to challenge the chair's ruling.

[*English*]

Frank Caputo: Nobody has challenged your ruling yet. You cannot challenge your own ruling.

The Chair: MP Caputo, I will—

Frank Caputo: I will challenge—

The Chair: Mr. Caputo, you don't have the floor. I have the floor.

Frank Caputo: I would ask for the floor, please.

The Chair: I am going to adjourn this meeting.