HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

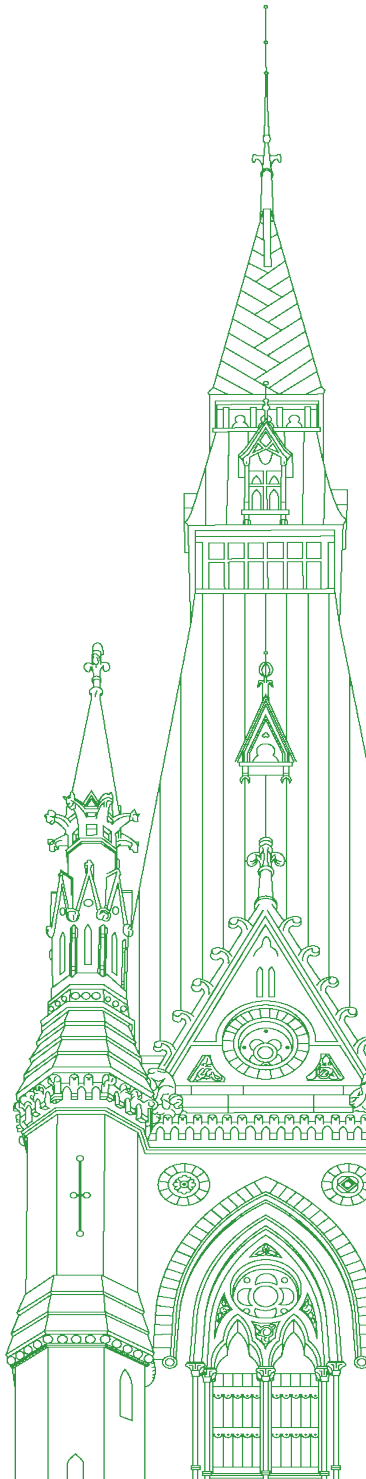
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 041

Thursday, June 4, 2026



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Thursday, June 4, 2026

● (1535)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): Hello everyone. Thank you for being here.

I call this meeting to order.

Welcome to meeting number 41 of the Standing Committee on Public Safety and National Security of the House of Commons.

Pursuant to the order of reference from the House made on April 20, 2026, and the motion adopted in committee on April 30, 2026, the committee is meeting for its study of Bill C-22, an act respecting lawful access.

I'd like to start by saying a few words to remind committee members about the process for the clause-by-clause consideration of bills.

As the name indicates, this is an examination of all clauses in the order in which they appear in the bill. As chair, I will call each clause one by one and each clause may be subject to debate before it is put to a vote.

If there are amendments to the clause in question, I'll recognize the member proposing it, who may briefly explain it, if they wish. Amendments will be considered in the order in which they appear in the package of documents that each member received from the clerk. Each amendment bears an identification number in the top right corner, which indicates the party that proposed it. During the debate on an amendment, members may also propose subamendments.

Amendments must be properly drafted in a legal sense and must also be procedurally admissible. The chair may be called upon to rule amendments inadmissible if they go against three key elements. First, an amendment may be deemed inadmissible if it goes against the principle of the bill or, second, if it is beyond the scope of the bill, given that the principle and scope of the bill were both adopted by the House when it agreed to the bill at second reading. Third, an amendment may also be deemed inadmissible if it infringes on the financial initiative of the Crown.

I thank the members for their attention and wish everyone a very productive clause-by-clause consideration of Bill C-22.

Now, I want to introduce and welcome the witnesses.

We have with us, from the Canadian Security Intelligence Service, Ramzi Nashef, director general, policy, planning and accountability, as well as Juanita M.

From the Department of Justice, we have with us Kimberly Gibner, deputy assistant deputy minister, and Normand Wong, acting general counsel.

From the Department of Public Safety and Emergency Preparedness, we have Richard Bilodeau, acting senior assistant deputy minister, Shannon Hiegel, director general, and Fenton Ho, director, intelligence policy.

Lastly, we also have with us from the Royal Canadian Mounted Police, C/Supt Richard Burchill.

On that note, we can start the clause-by-clause consideration of the bill.

Pursuant to Standing Order 75(1), consideration of Clause 1, the short title, is postponed.

We will go to clause 2.

(Clause 2 agreed to)

(On clause 3)

The Chair: In terms of clause 3, amendment NDP-1 is deemed moved pursuant to the committee's routine motion that the committee adopted on June 19, 2025.

Ms. Kwan, do you wish to speak to amendment NDP-1?

[*English*]

Jenny Kwan (Vancouver East, NDP): Thank you very much, Mr. Chair, and thank you for allowing me to present the NDP amendments on Bill C-22.

Relating to clause 3 and our amendment, I'll note that this is the government's second attempt at lawful access, after widespread outcry about Bill C-2, which the government was forced to abandon. Here we are again.

Some of the legal community's and civil society's concerns about part 1 were addressed, but I think it still misses the mark. With respect to the issue, I note that the Canadian Chamber of Commerce has raised concerns on behalf of its members with respect to the scope of and access to computer data. There are a number of legal experts, lawyers, scholars and business leaders alike who have raised these concerns as well.

To that end, this amendment would strike language permitting access to data “available to” a device, to ensure that warrants remain targeted and avoid broad or general searches of remote data. That's the element of the amendment I'm proposing.

The Chair: Thank you, Ms. Kwan.

[*Translation*]

I now turn the floor over to Mr. Caputo, who would like to speak.

[*English*]

Frank Caputo (Kamloops—Thompson—Nicola, CPC): Thank you very much.

Do we have all the briefs that were submitted translated, Mr. Chair?

The Chair: All the available briefs have been submitted, yes.

Frank Caputo: To be clear, because this is clause-by-clause, when I say that.... Various organizations and groups have submitted briefs to the committee. Have all those briefs been distributed? If a brief came in, do we have it now?

The Chair: Briefs were submitted yesterday. I would not be surprised if briefs were submitted today as well. There may be briefs submitted tomorrow. It is not possible for all briefs to be distributed immediately because translation needs to apply.

● (1540)

Frank Caputo: That's fair. I understand that. I'm not expecting a brief that came in yesterday to be translated by today.

I think it is fair that we know what briefs remain outstanding and what briefs don't. In other words, if a brief was submitted on Monday, hypothetically, do we have it today? If we're going through clause-by-clause and there were submissions made by stakeholders, we should know whether we have those submissions.

I hope I'm being clear in what I'm asking for.

The Chair: That's a fair question. The honest answer is that for this committee, as well as other committees, briefs follow the usual procedure. As we discussed last time, the House of Commons has resources that are necessarily limited. Things are allocated on the basis of the time they are submitted and the speed with which they can be translated.

Frank Caputo: I understand that.

Dane Lloyd (Parkland, CPC): I have a point of order.

The Chair: Go ahead, Mr. Lloyd.

Dane Lloyd: Would it be a good practice for us to get a list of outstanding briefs? I understand they might not be translated in time, but it would be good to get a list of the names of the briefs and who they're from. Would that be something reasonable for the chair and the clerk to provide to committee members?

The Chair: I can check that with the clerk.

I also need to check that with the other clerks—the usual procedures followed by other committees. We want this committee to follow not only the usual practice but also the best practice expected by the House of Commons.

Dane Lloyd: To continue on that point of order, Mr. Chair, I assume it is the best practice that committee members receive all the information necessary when reviewing a bill, especially during clause-by-clause.

I hope you will direct the clerk to expeditiously provide a list of outstanding briefs to our committee as soon as possible. I'm surprised we don't have them now.

The Chair: The clerk obviously wants to do his best. As I said, he will need to be assisted by other staff in the broader House of Commons.

Frank Caputo: I don't mean to belabour this, and I'm not trying to throw any shade at the clerk. I don't know how you would translate that, but I'm certainly not attempting to do that. We should know when we are going to have that information. We're about to embark on the first amendment. I don't want to hear a stakeholder say, “I have a point to make on the amendment, and I submitted a brief last Friday. That brief wasn't available, and now you are on the second NDP amendment.”

This is pretty serious. This is the federal legislature and we are dealing with a very contentious bill, with multiple motions on notice. I don't think it's unreasonable for us to know what information remains outstanding before we undertake scrutinizing and potentially changing this bill. A stakeholder may have proposed alternative wording, but we don't even know if they did so. If they did that yesterday, it's not a problem. I get that. If they did that last week or even Monday, however, I think we need to know whether it's outstanding. That's my position.

Mr. Chair, I can't tell you how to do your job. I can only give an exhortation. My exhortation is that we have the most fulsome information possible, and that information becomes possible with more information. I'll leave it at that.

The Chair: I think you have been very clear, MP Caputo. Thank you for that.

Ms. DeBellefeuille, do you want to say something?

[*Translation*]

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): I do not wish to speak in relation to the point of order but about the amendment, rather.

The Chair: Yes, you may speak about that, since you are next on the list.

Claude DeBellefeuille: Okay.

I have some questions for the officials so I can better understand the amendment. I think they're targeted more towards representatives from the Department of Justice.

If we were to adopt this amendment, would there not be a risk that evidence could be destroyed? Could law enforcement request a telewarrant for other devices once on site?

We have questions about the fact that evidence could be destroyed. I'm not sure whether you're able to answer my questions in detail.

● (1545)

Normand Wong (Acting General Counsel, Policy Sector, Department of Justice): Thank you for the question.

[*English*]

I think there is a risk that information will be destroyed. This articulation of the authority to search computer data and other data accessible to a computer system has been in the Criminal Code since 1997. The effect of this amendment, if passed, would be that it would actually make the job of police harder, which, I think, goes against the objective of the bill. They currently use this power routinely. In the Internet age, with cloud computing and other distributed networks, this is a very important tool for police to have.

[*Translation*]

Claude DeBellefeuille: I will rephrase my question to make sure I understand.

The idea is the following. Let's say, for instance, that police officers go to a home to seize a cellphone, for example, but are surprised to see another device of interest that they did not expect to see in that home. Clause 3 in the bill, as it now stands, would allow them to seize that device even though it was not originally targeted. As I understand it, the amendment would have the effect of restricting the seizure, so that police officers could seize only a device that was originally targeted. Did I understand correctly?

Normand Wong: Yes.

[*English*]

There are several ways that police can obtain evidence in a legal manner—I think you described some of them, and some of them are articulated in the amendments here—under a warrant. When they're in a premises, under a warrant, they can also seize other things that they think are associated with the crime, which I think you were talking about: other digital devices or other computers that are there.

These amendments are trying to treat all those digital devices the same. Under the current regime, because it wasn't designed for the seizure of computers, digital devices and the data on them, there's differential treatment in how those are seized, and that's not really sustainable in law. What this is trying to do is to ensure that, no matter how these devices come into lawful police possession, they're all treated the same. This is a tool that police can use to examine the data that's on those devices.

With regard to the amendment in question, the “available to” doesn't really have to do with this. This has to do with cursory searches or when police are actually examining the data and have the ability to go to a link where there are cloud services. They have the ability to search that data as well.

[*Translation*]

Claude DeBellefeuille: Thank you.

The Chair: Ms. Kirkland, you have the floor.

[*English*]

Rhonda Kirkland (Oshawa, CPC): Thank you, Mr. Chair.

I have questions regarding the amendment, but I just want to get some things off my chest. I promise I'll only take a very short couple of minutes. It won't be long.

I have a quick question for the chair before we proceed.

In the last meeting, you mentioned, Mr. Chair, that you would advocate for our committee in terms of getting the briefings and the timing, because this is such an important bill. I'm wondering if you've had an opportunity to do that.

The Chair: Yes, I have.

Rhonda Kirkland: Thank you.

Did it seem like there was going to be a bit more of a push to help us get all the documentation needed? It seemed as though it was going that way.

The Chair: Honestly, the answer is always balance, meaning that—

Rhonda Kirkland: I understand.

My background is in education. I have a very hard time studying something in depth unless I have all of the information at my fingertips, so I appreciate that.

Is there any way you can tell me how many...? Do you know approximately how many we're waiting on? Is there a guess? Are we waiting on 10, 12, 30 or 40? Do you have any idea of what we're looking at?

The Chair: No. I wouldn't be able to provide you with the number.

Rhonda Kirkland: Would the clerk know how many approximately?

The Chair: It's a fair question, but I think we want also to have an accurate answer. As I said earlier, the clerk, who is obviously listening, will follow up and not only provide that precise number, which obviously changes every day, I suppose, but also the way in which more information can be provided on the briefs that have been submitted until now.

Rhonda Kirkland: I appreciate that. I'm trying to manage my time, if that makes sense. If we were looking at 30 more that we're waiting for versus five more, it would help us manage our time.

You have no indication at all, not even a guess.

● (1550)

The Chair: It certainly will vary every day, because there is input and output.

Rhonda Kirkland: Of course. I mean as of now.

You have no idea.

The Chair: No, I wouldn't even....

Rhonda Kirkland: Okay. Fair enough.

As I outset all of my questions on the amendments that we're going to go through today and in the next sessions, I feel like I need to set the stage for all the questions I'm going to ask throughout the amendments. If you would permit me, I would like to qualify all of my questions based on this statement I'd like to give.

I want to begin where I think we have broad agreement. Conservatives have general support for part 1 of this bill. The testimony we've heard suggests that it has practical value. We can see that. It strengthens investigative tools and improves clarity in existing processes. There is a responsible path for part 1 to move forward, and I think Canadians would expect us to do that where there is consensus.

The question is whether we should treat part 2 in the same way. You've all heard my notice of motion. I do believe that we need to split the bill, but perhaps we'll talk about that down the road. I don't think we should treat part 2 in the same way, on the same timeline and with the same urgency. That is the precursor to all of my questions for amendments today. After all the testimony we've heard, I don't believe that we can responsibly say yes to that.

We heard from OpenMedia. Their warning was not abstract. It was pretty direct. Expanding lawful access frameworks and imposing system-wide obligations does not just affect individual cases. It changes the environment that systems operate in. It increases exposure. It increases risk. It increases the potential consequences when something goes wrong.

We also heard from Signal, one of the most trusted secure messaging platforms.

I promise that I'm just taking a couple of minutes. I really promise that, so please don't feel like I'm.... I promise you. It's just a couple of minutes. It will help preface everything I'm about to say for the rest of the evening.

Their message was stark: They would rather withdraw from Canada than be forced into compromising the privacy guarantees their users rely on.

We heard from a CSIS official that no technical system is ever fully secure and that lawful access mechanisms can potentially be misused beyond their intended purposes. I think we all know that. It underscores the need to fully understand all the risks as we proceed.

Even the public safety minister, when he was here, acknowledged that public trust does depend on Canadians' understanding of how their personal information is going to be protected in this bill. When that clarity is missing, confidence in both the law and its enforcement can begin to erode.

We also heard from legal and academic experts, who have repeatedly emphasized in public commentary and parliamentary testimony the importance of distinguishing between targeted lawful access and broader system-level obligations embedded in communications infrastructure.

Throughout the study, we've also heard concerns about how definitions and obligations in this bill may evolve over time through regulation—which I'm sure we'll hear more about today—and through ministerial powers as well. That raises a serious question about how much of this framework is fixed in legislation and how much is left to change after the fact without full parliamentary debate.

Mr. Chair, my concern is not that these questions exist. My concern is that we're being asked to move forward on part 2 without fully answering them. The technical adjustments go to the structure of how Canadians' private communications are protected.

I want to be clear. I don't want to slow things down: I want to not rush something. Once it's implemented, we can't undo it. I really truly, from my heart, want us to do this right. That's just why I wanted to predicate what I was saying. Canadians want us to move legislation forward, and I understand that, but we have to understand what we're changing before we change it.

Again, I will restate my position that splitting Bill C-22 isn't about delay. It's about responsibility, and it's about doing the job fully and not quickly. I do think we can do both, and I wanted to lay out my thinking as we got started.

I appreciated the questions that Ms. DeBellefeuille asked the officials.

Just to clarify, in a nutshell, if we were to adopt amendment NDP-1, would this have a great deal of impact on investigations? How much of an impact are we talking about this having on investigations?

● (1555)

Normand Wong: I tried to touch upon that. In this digital Internet age, when most computing has been distributed and much of it is outside of Canada, I think it would have a really big impact. The police have been using this power for many years now.

Rhonda Kirkland: How negative of an impact are we talking about?

Investigations are proceeding now, without lawful access. Would adding this amendment mess with this bill enough that it would make that huge of a difference?

Normand Wong: I think I'm going to ask the RCMP to answer this.

In terms of what this bill would do.... Since this bill is focused on giving the police new tools, this amendment would take away a very useful tool that the police have been using for almost 30 years now.

Richard Burchill (Director General, Technical Investigation Services, Royal Canadian Mounted Police): Thank you, Mr. Chair.

I have one of my colleagues here, Sergeant Aaron Gilkes, who's the current acting officer in charge of our national lawful access centre. I'd like to ask that he come in and provide Ms. Kirkland with some response to the question she's asking, to help clarify.

Essentially, if I understand it correctly, what the member is asking is how significant of an impact there would be on criminal investigations if this particular amendment were adopted. My colleague will try to provide some context in an operational sense.

Rhonda Kirkland: What I'm looking for is help in understanding exactly how this would affect it.

Aaron Gilkes (Acting Officer-in-Charge, RCMP Lawful Access, Royal Canadian Mounted Police): I appreciate the question, Mr. Chair.

Essentially, what we currently have is the ability to go on scene with a search warrant, and if there is a computer that is currently powered on, we can search that computer for what's contained within it.

There's a rather blurred line nowadays about what is contained on a device as opposed to what is accessible to a device. For example, with your mobile device, you may be looking at photos, thinking that they are contained on your device, but you're actually looking at just the thumbnails. When you click on the thumbnail, there's a download and you're able to see the picture that you think is on your device.

It's very much the same thing with a device that's in a home, for example. There are many types of computer systems that have a very small main hard drive. Most of the data is actually backed up on a cloud or in some accessible area. Having this ability to search that allows us to access that information before it could potentially be deleted. If there is more than one device that can access that cloud, for example, and it's in the possession of someone else who's off the premises, and they find out about the search before the police may be able to seize that evidence going further or to write a new search warrant, what could happen is that other person who has access could delete whatever information is there.

It's crucial to have access to that information and be able to seize it—with judicial authorization, of course.

Rhonda Kirkland: Okay. Actually, that brings up another question.

I have noticed this on my cellphone, for instance, with my contacts. They're all on the cloud now versus on my device. That has changed quite significantly over the most recent years. Is that correct?

Aaron Gilkes: Precisely.

Rhonda Kirkland: Thank you.

That answers my question.

[*Translation*]

The Chair: Thank you, Ms. Kirkland.

Mr. Caputo, you have the floor.

[*English*]

Frank Caputo: Thank you.

First of all, I'm a total nerd, especially on this subject. I'm going to give you one of my real-life examples, and we'll see if I'm getting this.

What we're talking about here is what is specifically on the system versus what is accessible to the system. Is that accurate? Okay.

One of the first cases of Internet luring that I dealt with was a very disgusting individual who was luring children from the Philippines. He was arrested for more substantive charges. Initially, it was a child sexual abuse material investigation. The RCMP got his hard drive and realized that, whoa, he was actually arranging offences in the Philippines. He was then arrested on that offence.

In the search incidental to the arrest, a cellphone was recovered, which was contrary to his condition on the original charge that he not possess any electronic devices. The RCMP did a data extraction, with a warrant. Within that data extraction were all sorts of Facebook communications.

Am I right to say that those Facebook communications would not be in the phone per se, but accessible to the phone? Is this the type of thing we're dealing with?

● (1600)

Aaron Gilkes: It's not that straightforward. It really would depend on the set-up of the individual themselves and where they want to keep their information. If it were accessible to something similar to a OneDrive, and they were to store their communications off of their device on that OneDrive and it would be accessible from any device they might want to access it from at a later date, that would be a good example. However, it's also possible that they could download those communications and keep them on their device, on a local drive within the device itself.

Frank Caputo: Right. My point is that within our devices we probably don't even realize what's there, most of us. For instance, I was just looking up an investment. I won't get into the details of things, but if it looks at my face and says my password is good, it can then access what's on that website. Is the current practice now to say that by having your device, we have access to what your device allows us to get to? In other words, that investment portfolio is password-protected. We get your password, which now gets us in there, but we have a judicial authorization, as in, a judge has said there are reasonable grounds to believe an offence has been committed and that there's evidence to be found in that place.

Is that where it gets us? I hope I'm being clear here.

Aaron Gilkes: That's correct. That would be accessible to you. You would be, essentially, in control of, in possession of the device itself—

Frank Caputo: Otherwise, a nefarious actor could simply store everything off of their phone. Unless you're a digital guru...which there are out there. There are people who are very careful. People who are nefarious are often very careful.

This is to prevent somebody from storing everything that is inculpatory, if you will.... If somebody were to store everything inculpatory and you were to seize their phone, if this amendment were to go through, you wouldn't be able to necessarily get the contents of that inculpatory information because it's held elsewhere, “outside” of the device. Is that correct?

Aaron Gilkes: You see that, for example, with a shared device. There's one family computer and an individual will not store the incriminating evidence on that device, but they will store it in the cloud and simply access it from the device.

Frank Caputo: That's also an interesting point, because there's a body of case law, as I recall, at least in British Columbia, that talks about waiver of charter rights. My understanding—and it's been a number of years—is that one person cannot waive the charter rights over another person's.... If a person has an expectation of privacy in a device and there is joint control of the device, person A can't waive person B's expectation of privacy.

Are you with me here so far?

Aaron Gilkes: Yes.

Frank Caputo: If this amendment was to not go through, could you have a situation in which there's a joint cloud, if you will, but you're dealing with the question of who has ownership of it? Would that come into effect as an expectation of privacy?

Aaron Gilkes: In this case, we're using a warrant to obtain that information, and I think what you're alluding to is more of a consensual search that's been provided by someone else who has control or who has access to the device.

● (1605)

Frank Caputo: Thank you. I think I have enough information to make a decision here.

[*Translation*]

The Chair: Thank you, Mr. Caputo.

Mr. Housefather, you have the floor.

[*English*]

Anthony Housefather (Mount Royal, Lib.): I just wanted to clarify, because I don't think this is so difficult. I wonder if you could just clarify, because I think this is the simplest....

There's a child pornography ring out there, and all of the members have access to a OneDrive where they store all of the child pornography materials. If this wording was changed per this amendment in NDP-1, you would not then be able to do anything, even though you have a thumbnail of the picture on the device. Is that correct?

Aaron Gilkes: That's correct.

Anthony Housefather: Okay, I think that is logical enough that, hopefully, everybody can vote now. Thank you.

The Chair: Thank you, MP Housefather.

[*Translation*]

Does anyone else wish to speak?

It does not appear so. Therefore, we will now vote on the amendment NDP-1.

(Amendment negatived [*See Minutes of Proceedings*])

The Chair: We are now at amendment BQ-1.

Mrs. DeBellefeuille, do you wish to move that amendment?

Claude DeBellefeuille: Certainly, Mr. Chair.

Our amendment came from the brief of the Barreau du Québec. Its objective was to add a guardrail to better regulate the extraction and examination of computer data. This was a recommendation from the Barreau du Québec, which drew our attention.

I am therefore proposing this amendment to committee members.

The Chair: Thank you, Mrs. DeBellefeuille.

Mr. Ramsay, you have the floor.

Jacques Ramsay (La Prairie—Atateken, Lib.): Thank you, Mr. Chair.

Respectfully, I would say that the ultimate aim of the bill is to expedite the process and ensure that investigations can be conducted in a timely manner and in real time. Rules such as those in this amendment will clearly result in much longer delays, which might even prevent investigations from being completed. It is a question of effectiveness. For that reason, we will be voting against this amendment.

The Chair: Thank you, Mr. Ramsay.

Mr. Caputo, you have the floor.

[*English*]

Frank Caputo: Could I hear from the officials?

One of the things is, “limited to the class of computer data specified”. Could somebody please give us different types of classes of data? Would that mean that every type of class would have to be enumerated within a warrant?

Does that make sense?

Normand Wong: Thank you for the question.

The description of class is no longer in Bill C-22. This articulation was actually in Bill C-2 when it was first introduced. I'm not sure what the Barreau de Québec intends here, but what we intended then was that the judge could impose the condition that the search can only go after photos, certain file types, email clients and things like that.

These are only examples of the conditions that a judge may be able to impose. That's what was intended back with Bill C-2.

Frank Caputo: Just so I'm clear, that's not what's here, but would this amendment restore that? Would it have to specify every type of data class of information that could be obtained?

Normand Wong: It would and, as you know, a series of consultations and round tables were held between Bill C-2 and Bill C-22. A lot of the stakeholders from the law enforcement side said that it's unnecessary. There's a variety of law enforcement stakeholders in Canada, like hundreds of police detachments of varying sizes that are resourced differently. It was felt that placing these conditions could become the norm, which would be inappropriate for some police detachments.

We still didn't want to remove the scope of the discretion of the judge to impose conditions that are reasonable in the circumstances, so that's why the new articulation is there in Bill C-22.

● (1610)

Frank Caputo: In these current circumstances, a judge still has discretion to put parameters on the type of data. It's not the de facto way. Do I have that right?

I'm just trying to get that through my head. I'm sorry.

Normand Wong: The judge has full discretion to impose any conditions he deems appropriate in the circumstances.

Frank Caputo: Would this amendment then narrow the judge's ability to impose those conditions, or would it fetter judicial discretion in any way?

Normand Wong: I think part of the issue with the amendment is that it really does not have any legal effect. Because of the way it's articulated in the motion, it's including these conditions, so it's non-exhaustive. These are just examples of conditions that a judge might be able to impose. I don't think it narrows it. It does nothing exactly to the scope of the conditions that might be able to be applied.

There is a risk that these conditions become commonplace because they're articulated and in the law itself.

Frank Caputo: Oh, I see. If a provision says that you need to look at X, Y and Z, then the industry practice becomes to include X, Y and Z because, as you said, it's non-exhaustive. If it's non-exhaustive, that means you can, as you said, include anything.

From what I'm seeing, there is limited practical benefit that may come, in your point of view, Mr. Wong, but it could add a layer of complexity down the road. I don't want to put words in your mouth. That's just what I'm taking from you.

Normand Wong: I think that's what we've heard from the stakeholders. They're afraid that these conditions may be imposed in circumstances when it's not appropriate just because they're articulated in the provision itself.

Frank Caputo: Thank you.

Those are my questions on that provision.

[*Translation*]

The Chair: Thank you.

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Actually, I was curious about something. Certainly, in my opinion, the Barreau du Québec is a good reference. After all, they're respected lawyers, particularly those who draft briefs.

What I find unfortunate is that we heard from the Canadian Bar Association, but we did not receive its brief or its proposed amendments. That's because there seem to be translation problems.

Therefore, I'm not sure what's going on. Was the Canadian Bar Association included in your consultations? I understand that you did not consult the Barreau du Québec, but was the Canadian Bar Association included in your consultations? I'm a bit surprised by what you're telling me.

What I understand is that the amendment would not change much. The parliamentary secretary said that the process should be able to be carried out in real time and that adopting my amendment would be very serious, yet you downplayed that. I believe you said that the amendment would not change much. That is my understanding.

Normand Wong: Yes. Thank you for the question.

Two weeks ago, when we spoke to the Canadian Bar Association, Bill C-22 was on the agenda, but they didn't give any—

Claude DeBellefeuille: They didn't elaborate on that, at least not on part 1.

Normand Wong: No, they didn't provide details on part 1.

Claude DeBellefeuille: That's fine.

Thank you.

The Chair: Thank you, Mrs. DeBellefeuille.

Shall BQ-1 carry?

(Amendment negatived [*See Minutes of Proceedings*])

(Clause 3 agreed to)

(On clause 4)

The Chair: We're moving on to clause 4.

Shall amendment BQ-2 be moved?

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Indeed, this amendment reflects the aim of the Privacy Commissioner to restrict information that could be confirmed without a warrant. He shared this intent with us. It's a way to restrict clients to telecommunications service providers. We therefore gave a voice to the Privacy Commissioner, for whom we have the utmost respect. He recommended that this information be restricted.

The Chair: Thank you, Mrs. DeBellefeuille.

Mr. Lloyd, the floor is yours.

[*English*]

Dane Lloyd: Thank you.

I thank my colleague for bringing forward this motion.

Conservatives also respect the work of the Privacy Commissioner. He's been here at this committee on a number of legislative studies, and we always appreciate getting his recommendations.

I want to ask this of the appropriate witnesses here today. What would be the impact of this amendment that would restrict seeking subscriber information from any “person” who provides a service to a “telecommunications service provider”?

● (1615)

Normand Wong: Thank you for the question. I'm trying to pull up.... Do we have the motion?

I'm trying to match the notes that I have in front of me with clause 4, which I think is the definition provision in 487.011. The definition here will apply to all of part XV. It has that knock-on effect of narrowing the scope of the production orders that mention telecommunication service providers. The confirmation of service demand will be focused on just them, but any other place where "telecommunication service providers" is mentioned will also be narrowed.

I think in terms of providing police with a useful tool, this will, again, narrow the utility of that tool.

[*Translation*]

The Chair: Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Mr. Chair, if I may, I would like a clarification.

I think that, based on what the Privacy Commissioner told us, the amendment relates to the order that requires a judge's consent.

Mr. Wong, I'm having a bit of trouble understanding the answer you gave to Mr. Lloyd.

Normand Wong: I apologize. I'm going to ask my colleague to send me the full text of the amendment, since I only have part of it in front of me.

[*English*]

As I mentioned to Mr. Lloyd, the narrowing of this—the addition of this inclusion—would also narrow the scope of the subscriber information production order. It has that knock-on effect. Currently, the subscriber information production order is servable on any person who provides a service to the public.

It's designed that way to ensure that police can obtain customer or subscriber information from any entity that might have relevant information for the investigation of a crime. The inclusion of this would also narrow the subscriber information production order. Because this comes up in the context of what I understand the amendment to be, how it works with the bill is that it goes into the definition section, so it has that knock-on effect.

[*Translation*]

Claude DeBellefeuille: In the Privacy Commissioner's speech, one of his arguments involved excluding certain sectors, like telemedicine, as well as information related to health and solicitor-client privilege. In his testimony, he referred to that.

I know that, further on in the bill, there are clauses dealing with that. However, if the definitions don't include restrictions, is it possible that confidential health or solicitor-client information could be accessed inappropriately, for example?

Normand Wong: Thank you for the question.

[*English*]

When Bill C-2 came out and there was concern around the scope of the information demand, which is now the confirmation of service demand, those concerns articulated by the critics were mainly related to the fact that it was a demand that police could issue on their own without any judicial oversight. This would form part of a Criminal Code production order, which is issued by a judge. The judge has discretion as to what is appropriate or not in the circumstances. Police, for a variety of reasons, may require information from all sorts of service providers, including hotels, car rental agencies, medical clinics and things like that, but in order to get that information they have to go before a judge and justify why they need it.

I understand what the Privacy Commissioner is trying to do because if you limit the class of people who can be served with this, you will restrict the amount of information.

The corollary to that is that there ends up being a differential privacy treatment of information in other service providers' hands. They either get more privacy or you'd have to use a tool like the general production order, so the people who have their data with those other service providers that are not covered...because this would narrow it. If it wasn't with the TSP, it would be under a general production order. The general production order allows police to access any and all information the service provider has on hand. It would almost have a negative effect, because the privacy would be more at risk. Police might just want to identify victims or people who are actually not persons of interest, but because they'd have to use that tool, they'd also be able to obtain all the information on them. The amendment is problematic from a number of perspectives.

● (1620)

[*Translation*]

Claude DeBellefeuille: To wrap up, I would like to thank you for speaking slowly, Mr. Wong. That way, the interpreter could keep up. You're a model witness. It's true. We're talking about highly technical matters, and often in English. I'm extremely grateful to you for speaking at a proper pace. I'm sure that we'll be hearing from you often. Perhaps your colleagues can learn from you. The pace was perfect. The interpreters could do their job and I could keep up with the discussion and, most importantly, understand you.

I'll tell you how I feel. Obviously, you didn't come here to tell us that our amendments that impose restrictions or that protect privacy are good. After all, you have the mandate to advocate for Bill C-22. Of course, as we study the bill, I don't expect you to say that our amendments do indeed protect privacy and should be adopted. I think that your goal is instead to give law enforcement more access. That's more or less the order that the minister gave you.

However, our job is to strike a balance. It may be restrictive, but we must ask ourselves whether these restrictions would be that serious. When we risk a failure to protect privacy, that too comes at a cost. Your responses show that you're a strong advocate for the need to give police forces access, but perhaps less so for the need to protect privacy. Throughout our study of the bill, if we're told that the proposed amendments wouldn't be that bad, but that they would prevent the police from doing their job, then this will be a fairly common response.

That's how I feel. I don't want to put words in your mouth, Mr. Wong. I'm telling you how I feel.

I gather that the amendment was proposed by the commissioner. His job is to protect personal information and privacy, so he'll obviously want to restrict lawful access.

I'm not sure that my amendment would have a major impact on police forces. I understand your explanation. I would still like to say that I get the impression that you're biased in favour of law enforcement, not privacy. I wanted to tell you that.

Thank you.

The Chair: Thank you, Mrs. DeBellefeuille.

Mr. Caputo, the floor is yours.

[*English*]

Frank Caputo: Thank you.

I note that Ms. DeBellefeuille said Mr. Wong was a model witness. She didn't call me a model parliamentarian, so I'm a bit hurt by that.

Voices: Oh, oh!

Frank Caputo: I'll move on to more important things.

The way we characterize the definitions in this section is actually pretty important. We're early on in the amendments, but this is a very important amendment, in my view, and a very important issue.

Right now we're talking about subscriber information that can be sought from a person who provides a service to the public. I think you touched on this. What categories could be included in that "a person who provides services to the public"? What could that include, please?

● (1625)

Kimberly Gibner (Deputy Assistant Deputy Minister, Policy Sector, Department of Justice): To answer and to add on to Madame DeBellefeuille's question, what my colleague was expressing is that the subscriber tool is judicially authorized by a court that balances both privacy interests and law enforcement interests. It's law enforcement versus privacy interest neutral, and it would apply to everyone. That is a really important point—to remember that this is a judicially authorized warrant for basic information like name and address.

As it relates to medical information, that provision doesn't speak to providing any content of anybody's service information, no medical information. Again, it's name and address.

In terms of the tool itself, it is a tool for law enforcement to investigate crime. Again, it's judicially authorized, so it has to balance those privacy interests. It's pretty straightforward. It would be everybody who provides a service. If a law firm is providing a service, a car rental, like my colleague identified, or any sort of service provider, law enforcement can go get a judicial authorization to ask the court for a court order to provide somebody's name and address.

Frank Caputo: I take your point about judicial authorization. I think the point that's being attempted to be made.... Perhaps I shouldn't be so bold. The point I will attempt to make is this. As I understand it, we are looking at a streamlined process in order to get information. Law enforcement has said, "We spend way too long getting really basic information," and this is why we use terms like "confirmation of service demand" rather than going out and getting things.

If, right now, we're looking at confirmation of service, my understanding was that the whole point of that was to streamline the process and, in so streamlining the process, it was to say the privacy interest that is being impugned or questioned is low. Asking, "Are you a customer? Are you this? Are you that?" is for the narrow category of service providers, so to speak. I think we were all thinking of the classic being the IP address, "Are they a customer of Bell?" When you start talking about streamlining getting information from a hotel, for instance, and things like that, I think that's a lot different. I'm mindful of questions such as, "Is this person a client of the hotel. Did they stay there or not?" To me, that's a much different privacy interest being streamlined than just, "Is this a customer?"

I hope I'm making sense here. How do you respond to that?

Kimberly Gibner: Again, the confirmation of service demand is scoped narrowly to telecommunications service providers, so you're 100% right. It's "Bell or Telus, is Kim Gibner a client of yours, yes or no?" That's a streamlined process. That is one tool.

The subscriber production warrant is also basic information—name and address—but because it's not just "Is Kim Gibner a client of yours?" but "What's Kim's address?" it requires a warrant. That is not just narrowed to telecommunications service providers, as this amendment is requesting us to do. It is currently drafted to apply to all people who provide services. They are two different tools and two different standards.

Frank Caputo: What's the different standard? I must be missing that.

Kimberly Gibner: The confirmation of service does not require a warrant. The subscriber production order requires a judicial authorization.

● (1630)

Frank Caputo: I see what you're saying.

Kimberly Gibner: One is very tailored. It's just to the telecommunications service providers: yes or no. You do not need a judicially authorized warrant. For the broader information, “What's Kim Gibner's address?”, you need a judicially authorized warrant. That applies to all people who provide services.

Frank Caputo: That judicial authorization is done in a streamlined manner. That's the whole point of this.

Kimberly Gibner: Yes, if by “streamlined manner”, you mean the test is reasonable grounds to suspect.

Frank Caputo: There's no prescription in terms of.... How would I put it?

Kimberly Gibner: There's no streamlined process other than the standard “reasonable grounds to suspect”, which is calibrated to the nature of the information.

Frank Caputo: It's commensurate with the diminished privacy interest.

Kimberly Gibner: Exactly.

Frank Caputo: We say that there's a reasonable ground to suspect, not a reasonable ground to believe, because we only want your name and address. Law enforcement should be able to get that based on suspicion, because all we're getting is your name and address. If we were getting your personal details, we would need reasonable grounds to believe.

Kimberly Gibner: That's exactly right.

Frank Caputo: Within that context—I guess I've spun myself into knots—how does this amendment change things?

Kimberly Gibner: This amendment wants to circumscribe this judicially authorized warrant tool to apply only to telcos, like the confirmation of service demand does.

Frank Caputo: If that's the case, if all we're dealing with are telcos, could you not just go and get a production order that says, “Give me Frank Caputo's name and address from the hotel he stayed at”? Could you not just do that? What's the difference there?

Kimberly Gibner: Again, just so we're using the same language, that's what this subscriber information is. It's a production order. The amendment is proposing that we go and get a judicially authorized warrant to get Mr. Caputo's hotel information—or whatever your example was.

If this amendment was passed, then law enforcement would be back to the reasonable probable grounds of the general warrant that we use to search your home in order to find out whether you rented at Hertz or Budget.

Frank Caputo: The status quo is a more arduous process. This is trying to—maybe “streamline” isn't the right word—simplify it.

The concern—I suppose—from the officials is that if we were to accept this amendment, we would be simplifying it in some respects but not in other respects. The status quo would still exist, which is a general warrant to go and search my house. I can't remember the analogy you used.

Kimberly Gibner: You have set that out correctly.

My colleague is just suggesting that it might be helpful for the committee's deliberations, if you want concrete examples, for the RCMP—

Frank Caputo: Concrete examples are always helpful.

Aaron Gilkes: In this case, if we're thinking about our grounds, at the beginning of an investigation.... I'll use an analogy. Basically, it's a very simple investigation that hopefully everybody will be able to follow to see the difference.

Take, for example, a stolen bicycle. Someone calls in and says that their bicycle was stolen and that their neighbour Phil stole it, because he told them he would. Now, there's no reason not to believe this person—who we're going to call Mike—who's declaring his bike has been stolen.

We're more or less at reasonable grounds to suspect. We can suspect that there's a bike that's gone missing. We can suspect that potentially there was somebody named Phil who might have been responsible for that. However, we haven't reached the threshold of reasonable grounds to believe, because we haven't confirmed or corroborated any of the information that's been provided.

Now, it's the same scenario. He came to the detachment and made the same declaration, but this time he showed text messages from his neighbour Phil saying he would steal the bicycle on Tuesday. He's also producing door-cam footage of someone who meets the description of Phil stealing a bicycle from his lawn and walking towards his own house on that Tuesday. When you do your police checks, you see that someone who lives beside the victim is named Phil. He has been known to steal and has been arrested seven times for stealing bicycles. His mug shot matches the description, or what you see in the doorbell cam.

● (1635)

Frank Caputo: This is interesting to me. We're going to be getting into the reasonable grounds to suspect and reasonable grounds to believe. If I've understood what you're saying, this all comes down to basically taking this down to the lower threshold of reasonable grounds to suspect for a certain class or a certain amount of information.

I'm sorry. I know Mr. Housefather was talking about just getting to it.

The whole reasonable grounds to suspect and reasonable grounds to believe discussion is going to occupy a fair amount of time of my questioning. I'll tell you that right now.

I know what reasonable grounds to believe is. In my view, reasonable grounds to believe is that you personally believe something—which is the subject of the nature of the belief as a police officer—and that belief is objectively reasonable. A reasonable person would also say that you have a basis on which to believe it.

Do you agree? It's been a while for me.

Okay. Can somebody help me? What does reasonable grounds to suspect mean legally?

I just laid out the legal test for reasonable grounds to believe. I don't know what it is for reasonable grounds to suspect. Can someone help us there?

Normand Wong: There is case law that talks about the reasonable suspicion standard. It's been described as a reasonable possibility instead of a probability. Reasonable grounds to believe is more of a probability, while reasonable grounds to suspect is a reasonable possibility.

Frank Caputo: That's interesting, because I always thought reasonable grounds to believe was not to the level of a prima facie case. For a prima facie case there is something there that you can get.

Maybe I'm just confused because this is a very technical area of law. When I think of something, it's that you have reasonable grounds to believe that an offence has been committed, and is that reasonable?

Mr. Wong, if I take your point, we're talking about "Has something happened? Yes, it may have happened." I suppose that's a bit inconsistent with my understanding, but I might be out to lunch on this.

Thank you very much.

The Chair: Thank you, MP Caputo.

[*Translation*]

Mr. Housefather, you have the floor.

Anthony Housefather: Thank you, Mr. Chair.

I'll try to speak slowly. I understand that it's difficult for the interpreters when I speak too fast.

[*English*]

I want to encourage everyone to use actual examples of how things work, because I think it helps us when you have concrete examples of how words will change the bill. I appreciate that we got to that point, but maybe that's a good starting point.

Here, I understand that if we change the wording to "telecommunications provider", we then no longer have the ability to use the lower grounds of reasonable belief to obtain a warrant and search.

For example, let's say we have a human trafficking case where you have a report that there's this middle-aged man with a young woman or a number of young women who has been staying at this hotel, went to this car rental agency and has this bank account, and you need to obtain quick information from the bank, from the rental car agency or from the hotel to try to find the victim who may be with this gentleman. You only have a report. You haven't done independent validation to get you to a belief standard, but you've reached the suspicion standard. Because of the way the law is now worded, you would be able to go to those different service providers, that are not telecommunications providers, to obtain important information, such as, "Are you a client of this bank? Were you at this hotel? Did you rent this car?" That's essentially the point of this, and that's what would change with this Bloc amendment.

I understand that we will eventually get to a profound debate about whether that standard should change, which I'm sure Mr. Caputo will, to use his words, "nerd out on", but for the moment, while we have the different standard in the bill, should we eventually remain with the reasonable belief standard, this amendment would thwart the intention of the bill to allow that lower standard for a number of service providers where you may need to obtain important police information.

Is that correct?

● (1640)

Kimberly Gibner: That is 100% correct.

Anthony Housefather: Okay. I know how to vote. Thank you.

[*Translation*]

The Chair: Thank you, Mr. Housefather.

Mr. Mantle, the floor is yours.

[*English*]

Jacob Mantle (York—Durham, CPC): Thank you, Mr. Chair.

Thank you to our officials for being here.

Mr. Wong, you made a comment during the discussion on the last amendment that I want to start with. It will be relevant to this amendment.

In discussing the previous amendment, you noted that it includes the word "including" and, therefore, in your opinion, had no legal effect. Did I summarize you accurately?

Normand Wong: Yes.

Jacob Mantle: You're familiar with the basic legal maxim that all legislation speaks. Is it not the case that when Parliament includes something in legislation a court is required—statutory interpretation 101—to consider that?

Do you want to revise your opinion that including the word "including" in legislation has no legal effect?

Normand Wong: I don't think I said it had no legal effect. I think the change to what the current wording was in the conditions, which gave the judge broad discretion to impose any reasonable conditions upon the search and examination of a computer, amounted to the exact same thing as the articulated examples of conditions, because the judge still has the discretion to impose those conditions if they so choose.

Jacob Mantle: Okay. It helps me understand where you're coming at this from, because I would certainly take a different view of that. For a judge considering a piece of legislation that has specific criteria, even if it is a non-exhaustive list, if they simply ignored that, I think that would be problematic and probably grounds to appeal that decision, so it's helpful to know where you're coming from. I'll come back to that non-exhaustive list issue in a second with respect to this amendment, BQ-2.

Ms. Gibner, you made a comment with respect to BQ-2 that in discussing subscriber information, it's only basic information. Am I quoting you accurately?

Kimberly Gibner: Yes.

Jacob Mantle: Could you tell me where in the clause of Bill C-22 that describes subscriber information it says that it's limited to only basic information?

Kimberly Gibner: The subscriber definition sets out exactly what it is, and that was my characterization of what that list is.

Jacob Mantle: If we go to that clause, I might ask you to bring it up so you have it in front of you. Let me know when you have it ready.

Kimberly Gibner: That's the definition of “subscriber information”. I have it in front of me.

Jacob Mantle: In proposed paragraphs (a), (b) and (c), as I read them, each of those paragraphs uses the word “including”, do they not? Proposed paragraph (a) says, “including their name, pseudonym, address”, etc. Proposed paragraph (b) says, “including account numbers”, and then proposed paragraph (c) says, “including” (i), (ii) and (iii), which are listed.

Is that right?

Kimberly Gibner: The word “including” is in all of those paragraphs, yes.

Jacob Mantle: As we just established, using the word “including” creates a non-exhaustive list. Is it not fair to say that in this definition, nowhere is it limited to, as you describe, only basic information?

Kimberly Gibner: My read, if it assists you in any way, is that the first part of the sentence clarifies the “including”. The “including” is giving examples of what the first part means. For example, in (a), it says, “information that may be used to identify the subscriber or client”.

That's the point of the sentence, in my opinion. Then they just give examples of how you might identify someone, for example, with their name, their pseudonym or their address.

I see those as describers, and I would characterize all of that information—this is just my characterization—as basic information.

● (1645)

Jacob Mantle: That's a significant difference of opinion, in my opinion, because when you use—

Kimberly Gibner: I missed the first part of your sentence. I'm sorry.

Jacob Mantle: I was just saying that I think we have a significant difference of opinion of what the drafting means, then, because the use of the word “including” has been litigated and is clearly understood to mean a non-exhaustive list. It's not just a list of examples.

I don't think that anything in (a), (b) or (c) is limited at all.

Kimberly Gibner: I agree with your general proposition about what the word “including” can mean, including how you described it with my colleague, but you have to....

You don't have to do anything—

Jacob Mantle: Give me your advice, though.

Kimberly Gibner: How I read the section starts with reading the chapeau too. It's pretty clear. It says it means this.

That's just my interpretation.

Jacob Mantle: Okay. That's fair. I guess we can have different interpretations, but this is why we're going through this, because, as I said, each word in a statute is important. There's nothing superfluous in law—that's another maxim. We'll see how many we can get in today.

I wanted to pick up on something you said, Mr. Wong, about this amendment. I think you said that regardless of what happens to this amendment, whether it's narrowed or not, there's still a general production order that can be sought.

Is that right?

Normand Wong: Yes, that's correct. The general production order is available.

Jacob Mantle: All right. I think you made the comment that these BQ amendments would weaken privacy. Am I capturing your thought accurately?

Normand Wong: Yes. I think the current scenario that we now live under, because there is no specific production order for subscriber information, means that any time police need subscriber information, the only tool they can use is a general production order, which gives police access to any and all information.

Jacob Mantle: When you go and get a production order, it's subject to the conditions that are attached to that production order by the court. Is that correct?

Normand Wong: That's correct.

Jacob Mantle: Is it fair to say that, in each case, those production orders can be limited as the court might determine on a case-by-case basis?

Normand Wong: They can be, but you're asking the police to jump through the hoops of getting a “reasonable grounds to believe” production order, which has a higher evidentiary threshold.

Jacob Mantle: I'm not arguing the threshold. I'm just arguing your characterization that these amendments weaken privacy because police would then have to go and get a general production order, and those can be for anything.

My point to you and my proposition is that it's not accurate because each production order, in fact, will be tailored to the request of the police. In each circumstance, it may not be just a blank cheque. In some circumstances it may be, but in many it won't be.

I can't speak from experience on that. Maybe the police can offer their views, but I think as a proposition, that's not accurate.

How do you respond?

Normand Wong: I respectfully disagree.

These tools have been designed.... You can think of the general production order as a fishing net. The fishing net grabs anything and all that's in the sea. The specific production orders are like jiggers or fishing rods; they're designed to catch specific fish. If the only tool you have is a fishing net, then you catch whatever. To ask police to jump through the evidentiary burdens of meeting these things.... They'll ask for everything, just in case they need the information later, just in case that person ends up becoming a prime suspect in the investigation.

Jacob Mantle: Okay. Thank you.

I think, in fact, you're actually making the point that the Privacy Commissioner made, which is that the broadness of the definition, the broadness of whom these apply to, is the problem. To me, you're just confirming that problem.

These amendments are trying to narrow that and maybe make it—to use your analogy—a smaller net.

The Chair: Thank you very much.

● (1650)

[*Translation*]

Before we proceed to a vote on amendment BQ-2, let me inform you that, since amendment BQ-2 has been moved, amendment CPC-1 can't be moved given that the two amendments are identical. Furthermore, if amendment BQ-2 is carried, amendments BQ-3 and CPC-2 can't be moved because of a line conflict.

I'll remind you of the definition of a line conflict. Once a line of a clause has been amended by the committee, it can't be further amended by a subsequent amendment. In other words, a line may be amended only once.

So, now that I've given you this information, shall amendment BQ-2 carry?

[*English*]

Frank Caputo: I would like a recorded vote, please.

[*Translation*]

(Amendment negatived: nays 6; yeas 5 [*See Minutes of Proceedings*])

The Chair: Since amendment CPC-1 is identical to amendment BQ-2, we'll move on to amendment BQ-3.

Is amendement BQ-3 so moved?

Claude DeBellefeuille: Yes, Mr. Chair.

Again, this amendment is based on a recommendation from the Privacy Commissioner. I gather that his intention in this case is to slightly restrict subscriber information.

Mr. Wong, I'm not familiar with all the English phrases used earlier. Please understand that it's important to us that this bill doesn't give police forces a large fishing net. There must also be certain restrictions, so that the police forces don't have total freedom to breach privacy.

That's my proposed amendment. The amendment isn't that restrictive. The French version includes the word "*notamment*", which means that the judge still has discretionary power. It's nonetheless important to point out that we don't want these measures applied in a broad and unrestricted manner. Instead, we want the subscriber information restricted.

I hope that my colleagues will support my amendment.

The Chair: Thank you, Mrs. DeBellefeuille.

I would like to inform you right away that, given that amendment BQ-3 has been moved, amendment CPC-2 can neither be moved nor considered, since it's identical to amendment BQ-3.

Ms. Kirkland and Mr. Caputo would like to speak.

Ms. Kirkland, you have the floor.

[*English*]

Rhonda Kirkland: Thank you. I appreciate this.

Madame DeBellefeuille said something very important as we were listening to the department officials. I appreciate that you're answering a lot of very technical questions, and you're doing the best that you can, but she was right when she said that your job is to give more access to law enforcement. I mean, the purpose of this bill is to give more access to law enforcement, but our job is to balance it, truthfully, with Canada's charter and rights to privacy. We really have to do that. I would hope that you consider those things as well, as we ask those questions, and not just the one side of things. I guess that's all I'll say on that.

Anyone can answer—whoever. Is it fair to say this amendment improves...? I mean, I think it improves legal precision. Is that not right? It ensures that only clearly identifiable information is captured rather than broad or potentially ambiguous data types. Would you say that's fair, or do you have anything to add?

● (1655)

Normand Wong: Thank you for the question.

Keeping with my previous intervention, I think, in a non-exhaustive list, this has limited legal effect. Removing it doesn't mean that someone might consider the pseudonym as part of the subscriber information they might be able to provide. I don't think it does much one way or another, legally.

Rhonda Kirkland: I'm sorry, but could you clarify that very last thing you said—that it doesn't do anything much one way or the other?

Normand Wong: Yes, it's because this is a non-exhaustive list of potential identifiers that can be ordered. The way that it's drafted now, removing "pseudonym" from there would be less instructive, but that doesn't mean that a judge could actually order pseudonyms to be produced if the service provider had them on hand.

Rhonda Kirkland: I'm sorry. I'm just trying to wrap my head around.... Does removing pseudonyms from the definition then strengthen the principle of data minimization by ensuring that only necessary and clear attributable information is included? That's how I'm seeing this.

Normand Wong: I think the reason it was included is that there is a need for it, sometimes, depending on how someone has set up their account. If you set up your Instagram account and you characterize yourself as “Daffy Duck”, and Instagram had information on Daffy Duck, they'd be able to provide that. This is why it was added. Whether or not that leads to data precision in terms of privacy safeguards, I think is debatable. What the tool is trying to provide is information so that police can identify suspects.

Rhonda Kirkland: In a nutshell, you're saying that this amendment doesn't reflect a balance between.... I'm trying to get to the point at which we're looking at balance—a balance between effective investigative capability and also stronger privacy protections for individuals using telecommunications services. With that balance in mind, if it doesn't matter one way or the other, then we might as well preserve as much privacy as we can. Is that not right? Am I completely misunderstanding where you're going with this?

Normand Wong: Perhaps...or I'm misunderstanding.

I think, again, that the elements in the subscriber information definition were there to give examples of the types of information police need during an investigation in order to identify criminals. The reason they're included is that there are real-life examples in which they might have to go after a pseudonym or they have a suspect and they know this person via an IP address, and that's why they've gone to Rogers, for example, and asked for the subscriber information. If Rogers has on hand any pseudonyms that the client used on their services that are registered with them—for example, email addresses they might have registered with them—then it could provide those.

Rhonda Kirkland: Mr. Gilkes, let's talk about concrete, real-world examples. Can you give us a couple of different examples, so that we can really wrap our heads around this?

Aaron Gilkes: Absolutely. We have to keep in mind that we're police, so we're investigating criminals most of the time. We do also investigate missing people and things like that. If we are investigating criminals, then likely they're not going to want to use their real identities when they're registering for various services, especially if they're going to be committing crimes online.

As this is the case, some of the time we have to use other ways to identify the people who could potentially be behind whatever crime we're investigating. We may be asking for information that very much differs from service provider to service provider. We don't know exactly what is required to create each account or whether there are monikers that can be created and associated with a name that has been associated with the creation of the account. Somebody may have multiple accounts associated with a particular name, whether they're called handles or whether they're temporary or permanent and things like that.

This is information that can be provided to police, which can help them link these individuals to other platforms and to previous registrations in other places. Those police officers can then continue with additional judicial authorizations to obtain additional information.

● (1700)

The Chair: Is that all right?

Rhonda Kirkland: I think so. I don't feel at all confident in all of the answers. I'm getting there. Do you have any other examples you want to give?

Maybe Frank can help me clarify my thoughts.

The Chair: We'll go to MP Caputo.

Frank Caputo: I think what this comes down to—if I have it right, and maybe I don't—is that if the Privacy Commissioner says you shouldn't include pseudonyms, that's the recommendation, but the police are saying that including pseudonyms will help them catch criminals.

Perhaps I could ask this. Could someone finish the following sentence? Including pseudonyms will help us catch criminals because....

Please, go ahead.

Kimberly Gibner: Criminals use pseudonyms.

Frank Caputo: Okay. I think we need to go one step further. I have a great deal of respect for you, Ms. Gibner, and I know you really know your stuff. I understand that criminals use pseudonyms. I don't have a burner account. I'm very proud of that. A lot of politicians do. I do not have any burner accounts with which I attack political opponents.

Why are you laughing, Mr. Housefather? Do you?

Anthony Housefather: I definitely do not.

Jacques Ramsay: I didn't even know it was possible.

Frank Caputo: You didn't know you could have a burner account, Mr. Ramsay. Good grief—I don't know if I buy that.

People use burner accounts, obviously, or pseudonyms. Pseudonyms are used in order to not identify yourself, if we're being candid. Is your point that we want pseudonyms simply because that might be akin to a username? “Frank Caputo, MP” is my username, but somebody else might use “Daffy Duck” as their main thing.

Why is that necessary? Why can't we get the person's information without the pseudonym? That would be the logical point. I think I know the answer, but I think we need to flesh that out based on what Ms. Kirkland was getting at. I think that was the point she was trying to get to.

Kimberly Gibner: I'm going to go back to the point I made earlier. This is a judicially authorized warrant. Police are going to go with the evidence. Either they're going to go with Daffy Duck or they're going to go with an IP address and say, “I need it associated.” The purpose of the tool is to connect the first initial dot at the beginnings of an investigation. The police don't know what they don't know. The definition is set out for the various things they've come across in real life, and we've articulated that in law to be as clear as possible. First principles are that they're going to have to go to a judge with some evidence in order to get it authorized.

Frank Caputo: The evidence would be predicated on connecting the dots. If I take your point correctly, the dots don't get connected if we don't have the information, and the information we need is sometimes in the form of a pseudonym. Is that the point?

Kimberly Gibner: My point, again, is that I think it's really helpful to the committee to hear examples. If Mr. Gilkes has an example of a pseudonym that sort of connects the dots for us all here, maybe that would be helpful to the committee.

● (1705)

Frank Caputo: "Muscleman Frank" or something like that is a very good place to start, Sergeant. I'm being facetious here.

Let's ask this. What percentage of people in your investigation use it for child luring and things like that? In my experience, a lot of people use pseudonyms, but a lot of people don't. A lot of the time, when you get a report, for instance, that says this is the person, they will have often logged in with their real name or their Facebook is tied to their actual email address that might be frankcaputo@rogers.ca or something like that.

Do you get what I'm saying, Sergeant?

No, that is not my real email address. You're going to get bounced if you try to email that.

Anthony Housefather: Millions of Canadians are sending you emails right now, Frank.

Frank Caputo: That includes Mr. Housefather's burner account.

Sergeant Gilkes, can you elaborate on what I've said? How often does it happen that the pseudonym is so important to an investigation that it's absolutely necessary?

Aaron Gilkes: I don't have exact numbers.

Frank Caputo: Anecdotal is fine, just in your experience.

Aaron Gilkes: Anecdotally, I've investigated many different types of crimes, whether they be financial or cybercrime investigations. Depending on the type of crime being committed and depending on how widespread the crime is, that's when it comes more into play.

I'll give an example. In cybercrime investigations, there's something called pride. A lot of the time, cybercriminals start off as gamers, and they are particularly good at a particular game. This is something that may come back later on. They may use a moniker that they used many years ago, because they're proud of what they've accomplished in a certain game. That name may be used sometime later when committing an offence, and you're able to link the name that's being used sometime later to an account that was created years before in a particular game. That gives us some insight as to who might be behind the offence.

Frank Caputo: That I can understand.

In your experience, is this a frequent thing? People might use a moniker or a name from the past, a reference to gaming, high school, being a good skateboarder or something like that.

The question I'm trying to get at is this: In your experience, is that very frequent, sometimes occurring or seldom occurring? That's what I'm trying to get at. Again, you can only speak to your experience. I'm not trying to qualify you as an expert here. What I think the committee is asking for you to explain is how often this happens.

Aaron Gilkes: Particularly in cybercrime, it does occur often, because you're dealing with an anonymous space. For example, you'd be dealing on the darknet. The whole purpose of dealing on the darknet is to avoid detection and remain anonymous.

That helps, in terms of a lead, when you're operating in this type of space, to potentially target an area where you can accumulate additional information or additional evidence to help prove your case.

Frank Caputo: That doesn't mean that you couldn't go and get a production order at the higher standard of reasonable grounds to believe for the pseudonym, does it? You're not precluded from doing that. Is that correct?

Aaron Gilkes: You're not precluded from doing that, but the issue is at what stage of the investigation you can go ahead and obtain that information.

Frank Caputo: You're saying that because at one point in the investigation, you may not be at reasonable grounds to believe. You may still be at the lower threshold. Is that accurate?

Aaron Gilkes: That's correct. One of the obligations that we would have, if we were going to obtain a general production order, would be to establish and show to the judge or justice, whoever is approving, that the person or the entity that you're requesting the information from is actually in possession of that information, which you need to confirm before you can go ahead and obtain your production order.

Frank Caputo: This is all about grounds and the difficulty with grounds—or much of this is, really.

Aaron Gilkes: For us, yes, it's expediting the beginning of the investigation, because that's where an investigation is more crucial to get off the ground.

Frank Caputo: It's interesting because the reasonable grounds to suspect, which Mr. Wong told us about earlier, and the reasonable grounds to believe are common law doctrines. Forgive me and tell me if I'm wrong, but none of that.... Is that anywhere in the legislation? When I gave that definition of reasonable grounds to believe, that was my recollection from a case called Storrey, which is from the mid-1990s about whether you have grounds to arrest. Is that enumerated anywhere in law?

I'm not going to look at you, Sergeant Gilkes.

Maybe that's something we as Parliament should actually be addressing. If we're talking about grounds to suspect and grounds to believe, the common law can change. Maybe this is something—I'm just thinking out loud—that we as parliamentarians should be considering: whether we need to codify what these grounds actually mean.

That may be neither here nor there. I'm sure Mr. Mantle has far more interesting things to say than I do, so I'll pass the floor to him.

● (1710)

The Chair: Before we do that, I will list the names of those who I have already. We have Mr. Mantle, Mr. Ramsay, Madame De-Bellefeuille, Mr. Housefather and Ms. Kirkland.

Given that we're at more than half time, I will suspend for five minutes so we can stretch a little bit. Don't go too far. We'll start again in about five minutes.

● (1710)

_____(Pause)_____

● (1715)

[*Translation*]

The Chair: We'll now resume the meeting.

Mr. Mantle, you have the floor.

[*English*]

Jacob Mantle: All right. Thank you, Mr. Chair.

I wanted to return to the idea of basic information that Ms. Gibner brought up. We're dealing with a list of identifiers, if I can use that word, for what constitutes subscriber information. In your mind, are there any categories or classes of subscriber information not currently listed here?

I guess that's an open question for either yourself, Ms. Gibner or any of the law enforcement witnesses or officials. We were talking about pseudonyms and other things.

Are there other classes that you've dealt with here that are not listed?

Normand Wong: Thank you for the question.

The subscriber information definition is based on international standards and all the work that has gone on in the international community to describe these things. Proposed paragraphs (a), (b) and (c) are supposed to cover the types of information that will be of use to police. That's why they are described the way they are with the examples after. It's to try to make them future-proof in terms of what other types of information.... For example, there's information that may be used to identify the subject and then it gives a list of examples, identifiers assigned by the service provider with a list of examples, etc. The idea is to try to be as comprehensive as possible.

● (1720)

Jacob Mantle: Good. I was thinking that it would be the case that this list is comprehensive.

I understand that we're dealing with the BQ amendment, which came from a recommendation from the Privacy Commissioner. If this list is comprehensive, as you say, what would be the effect of defining it as such—just defining the list?

Normand Wong: The list sort of works both ways. The chapeau says “means”, which is usually a defined list. The first part of proposed paragraphs (a), (b), and (c) is supposed to be what subscriber information means. If you read each paragraph without the “including”, that would be your defined list. It's any of the information that does these things. That's how it should be read.

If you're talking about naming specific identifiers, like a closed list of specific identifiers, I think it wouldn't be future-proofed, and we may be back here in five years to amend this section again.

Jacob Mantle: Okay. I assume you're implying that it's a less desirable outcome to come back to Parliament if there are changes that need to be made after this is passed or not passed. Let's assume for argument's sake that it is passed as a finite list, and then, through experience, new categories emerge or new technology emerges and you have to come back to revise it. Are you suggesting that's a less desirable outcome?

Normand Wong: Whether or not it's a desirable outcome, that's the drafting tradition that we use in the Criminal Code—to try to be neutral in language and explain what we want from a provision without being technology-specific. That way, the code doesn't have to be changed every so often.

Jacob Mantle: Okay.

To the law enforcement colleagues, on my original question, from your experience or your collective experience, are there things that are categories or classes of identifying information that you may have dealt with or may need in the course of your duties that you don't see reflected here?

Aaron Gilkes: In a short answer, I think that the categories cover most of the identifiers that I would look for. Once again, that's with minimal revision in a few seconds here.

Jacob Mantle: That's helpful.

I hope it's not minimal review. You've been looking at Bill C-22 for a while now.

Aaron Gilkes: Yes. I just haven't considered it in that light, where there might be something that hasn't been listed.

Jacob Mantle: That's fair enough. It's always harder to show or prove the negative. I take that as well.

One of the supporting factors that the Privacy Commissioner made in suggesting this is that—to take your point about previous drafting or the tradition of drafting, Mr. Wong—the narrowing of "subscriber information" in the manner suggested by the Privacy Commissioner was actually similar to a previous proposal in Bill C-30 in the 41st Parliament.

Why, in your view, was it...? Maybe it's an unfair question. I don't know if you were there in 2012.

Normand Wong: I was there.

Jacob Mantle: All right. It is a fair question. Excellent. I gave you an off-ramp and you didn't take it. This is on you then.

Why was that approach the right one? It was proposed but now it's not, and you're going with something different

● (1725)

Normand Wong: Thanks for the question. I have a good answer. That's why I didn't take the off-ramp.

Bill C-30 proposed an administrative scheme for subscriber information. There was no requirement for judicial oversight. It was scaled back for that reason. There were other checks and balances that were built into that legislation. It was not enacted.

Since we have to go before a judge now with a production order and the judge has the discretion for granting the order or not for the subscriber information, the decision was made that this was the check and balance against that. That's why it was expanded.

Jacob Mantle: Okay. Perfect.

Maybe this is an unfair question, then.

That's a reasonable response. If you have an administrative scheme, then it can be modified more easily than having to change the law. I think that's what you're saying.

Normand Wong: No. The administrative scheme was a statutory scheme that was proposed, so it would have been difficult to change as well.

Jacob Mantle: My question stands, then. Why was the definition of "subscriber information" the right approach then, but it's not the right approach now?

Normand Wong: It was a statutory administrative scheme. It was in law. The scheme required oversight from a senior police officer. There was auditing involved, but there was no judicial oversight. There was no need to go to the court. Any police detachment could probably poll the system directly from their police department and obtain the information. That's how that scheme worked.

This scheme requires the police to go to court to get a production order for this information. I'm sorry if I'm not explaining that right.

Because there was no court oversight, the definition of "subscriber information" was scaled back. Because there is judicial oversight now and the discretion goes to the judge for whether or not it's issued, it was expanded.

Jacob Mantle: Okay. I see what you're saying. You were more comfortable having it in an expanded manner here because of that judicial oversight. I guess that's a slightly different question from what we were previously discussing, which is whether there may be a necessity to update a defined list in the future, based on whatever changes may take place.

Normand Wong: That's right.

Jacob Mantle: Thank you for those comments.

I may come back to this issue, but those are my thoughts for now.

[*Translation*]

The Chair: Thank you.

Mr. Ramsay, you have the floor.

[*English*]

Jacques Ramsay: I think we've established that the objective of this amendment is to replace a broader definition of "subscriber information" with a narrow list of identifiers.

When I look at the conditions of a production order, my understanding is that not only does an offence have to have been committed or will be committed in the future, but we also need to establish that the subscriber information will assist in the investigation of the offence.

Consequently, am I right to assume that a judge will not authorize the release of that information unless the requesting party can prove it will be useful? That would be my first question.

Normand Wong: Yes. The affidavit has to demonstrate all of those conditions you mentioned. In addition to that, the construction of the production order for subscriber information also requires the police to have an identifier that the subscriber information relates to. It's even more limited in terms of how it's constructed. The police have to be seeking the subscriber information that relates to specific information already in their possession or control.

Jacques Ramsay: Am I right to argue that it would probably be better to leave it for the judge to decide because he knows the particulars of each case and he is more apt to decide what information should be in the production order rather than the legislator trying to assess any case that could happen under the sun?

● (1730)

Normand Wong: That's how the production order was designed. Getting back to the previous question, because the judge has discretion to order the production of the subscriber information, we think that they're the best place to assess that based on the evidence produced by the police.

Jacques Ramsay: That's all. Thank you.

[*Translation*]

The Chair: Thank you, Mr. Ramsay.

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: First, I would like some clarification.

I gather from the Privacy Commissioner that, since the threshold for obtaining information is low, it may be too intrusive to go looking for information on the services received. That's why he recommended this amendment to protect privacy.

We've been talking a great deal about pseudonyms. However, do we really need the list of all the services received? That's what we need to ask ourselves. That's the idea behind my amendment. Is it really that vital? Where do we draw the line in terms of allowing police officers to do their job while ensuring a certain level of privacy? If the threshold is low, where's the balance?

Furthermore, the amendment isn't phrased as an instruction or order. It's intended for information purposes.

For example, I don't understand why we would keep the whole issue of the information obtained on the services received. It's a big fishing net. If my amendment were carried, would it really prevent the police officers from doing their job? Of course it would be more difficult, but it wouldn't be impossible.

Again, Mr. Wong, we're looking to strike a balance. I currently feel that it's quite broad. Yet the commissioner is telling us to be careful. Maybe it's possible to go looking for the information based on the lowest threshold, but do we need to go this far? That's my understanding of the commissioner's comments. He's wondering whether we need to go this far.

I know perfectly well that, after my comments, the vote will likely take place and the amendment will be rejected. Yet we aren't looking to filibuster today. We're looking to strike a balance. I thought that the compromise recommended by the commissioner could satisfy the police forces while placing a certain restriction and a certain limit on access to certain data, including data on the services received by the subscriber.

Normand Wong: Thank you for the question.

[*English*]

I have a comment on that in terms of how the definition is built. With some of these categories, especially (c), because the amendment is asking for the repeal of proposed paragraph (c), that type of information is already available when it's considered transmission data under the transmission data production order, which is already at reasonable grounds to suspect. Some of that data is already analogous to other data that is in current production orders. In terms of trying to be consistent in the Criminal Code and not having different legal standards or standards of review for the same types of data, we included it here.

[*Translation*]

The Chair: Thank you, Mrs. DeBellefeuille.

Mr. Housefather, you have the floor.

Anthony Housefather: Thank you, Mr. Chair.

[*English*]

I think we're again introducing a whole lot of complexity to this amendment.

If I have it straight, this amendment has two parts. The first part is deleting the word “pseudonym” from the list of things that are included, which means we're essentially debating whether or not we remove the word “pseudonym” from an inclusive list, which could include other things that are not enumerated on the list.

Would I be right about that, Ms. Gibner?

● (1735)

Kimberly Gibner: You have that right, sir.

Anthony Housefather: Okay.

Then, as for a pseudonym, does anyone remember Karla Homolka, the wife of Paul Bernardo? I believe she went by Leanne Teal. Would that be a pseudonym for Karla Homolka?

If Karla Homolka, for example, in the old days when you used to develop pictures, had gone to a photo store and, let's say, they had this information online or wherever they kept it in their records, and instead of using “Karla Homolka” to develop the pictures she took at the crime scene when these poor girls were being victimized she used the name Leanne Teal, I would assume that maybe it would be more difficult to get the information than if she had used her real name of Karla Homolka.

Would that be correct, if you remove the word “pseudonym”?

Kimberly Gibner: If that question was for me, that would be my understanding. I think that's what I heard.

Anthony Housefather: Yes, my questions are for you until I say otherwise. So far, you've been very good at giving me short and clear answers.

This is the other question I have: Why would a pseudonym be more important to my privacy interests than my own name, my own email address and my own telephone number? It seems incredibly odd to me that we're having this whole argument about whether a pseudonym—a fake name that I intend to use—somehow gives me greater privacy rights than my actual information.

Do you not find that a bit weird? I see you're nodding, so maybe you want to—

Shannon Hiegel (Director General, National Security Policy Directorate, Department of Public Safety and Emergency Preparedness): No, I suppose I don't, because I've worked with law enforcement for many years now. As the online environment has just exploded...we all do it. I do it. I smile because I know for my first email account when I was 15, I didn't use my name because I didn't want it connected with me.

That's just a little personal anecdote there.

Anthony Housefather: That's fair. Again, it seems to me that your name is more important than your pseudonym, so I don't understand that whole part.

The second part of this seems to be to remove the words “the types of services provided” and “the period during which the services were provided”. Again, if I were to go to that photo store, I wouldn't be able to find out, at this lower threshold, whether or not she had photos developed. That's the whole amendment.

I'm not really understanding why a pseudonym, the types of services I provided or the period during which the services were provided somehow carry higher privacy rights than the other enumerated parts of this section, where we describe and explain what subscriber information is.

I guess my point is that I'm voting no. My other point is that I don't understand how this is so complex. I think I was able to boil it down into two parts in about seven seconds.

Thank you.

[*Translation*]

The Chair: Thank you.

Ms. Kirkland, you have the floor.

[*English*]

Rhonda Kirkland: Thank you. I appreciate that. I will not be daunted by the idea that asking good questions is silly.

Mr. Wong, you mentioned something a little while ago that I wanted to pick up on, which is why I got myself back on the list. You said something about future-proofing, and I wonder if you could clarify that. I think that was the term you used. Correct me if I'm wrong.

Normand Wong: That was the term that I used.

Rhonda Kirkland: Can you clarify what you mean by that?

Normand Wong: The convention in the Criminal Code is to use words that describe what we want it to achieve or the types of services without naming the services. One of the things that we did back in Bill C-13—I don't remember which parliament that was—was to remove the word “telegraph” from one of the provisions in the Criminal Code, because no one uses a telegraph anymore. We replaced it with something akin to “means of telecommunication”, which covers any sort of mode of telecommunication.

This is what we generally mean when we talk about future-proofing. We use general language that actually gets to the heart of the criminal behaviour, and we do not specify the mode used to accomplish it.

Rhonda Kirkland: If I'm going to be honest with you, though, that term is really what stops me and makes me pause.

How difficult was it to amend and remove the word “telegraph” in that example you gave?

● (1740)

Normand Wong: It seems difficult for any piece of legislation that I work on, so I would say it was quite difficult.

Rhonda Kirkland: Is it safe to say that you're always on the difficult legislation? It seems like it.

Normand Wong: I work in the area of investigative powers, so....

Rhonda Kirkland: For safety and security, quite frankly, I would think that the way we protect Canadians' privacy is to do what is needed at the time. Should amendments be needed five years from now, we would address that need at the time. I think that's why the Privacy Commissioner made these recommendations.

I have a great deal of respect for what the Privacy Commissioner has said and what he has proposed. I don't think Mr. Housefather meant to make it sound like the Privacy Commissioner was being silly by his not getting it in terms of the recommendation, because I would find that quite offensive.

Let me do it this way. I am going to ask this question, and I would love to have an answer from each of you, including Mr. Nashef from CSIS, Mr. Wong and Ms. Gibner.

Mr. Gilkes, perhaps you might have input on this as well.

It feels as though your job here is to explain to us why we need to provide lawful access and much more lawful access. We want to give access to law enforcement. That's the deal here, but we have to balance that. That's our job. We have to consider charter rights and the expectation of privacy.

With that and with the Privacy Commissioner having made these specific recommendations, if this amendment is so difficult and puts up such a barrier and such a roadblock to lawful access, I would ask each of you to tell me why you think the Privacy Commissioner has suggested it.

Ramzi Nashef (Director General, Policy, Planning and Accountability, Canadian Security Intelligence Service): I wouldn't want to speculate on his specific motivations.

To circle back to Ms. DeBellefeuille's framing earlier, which I think was helpful, I think that reasonable people coming from different perspectives could try to strike the balance between privacy and security in different ways, and I think we're all trying to do that and get it right.

I might add one line from our perspective. I take her point that we're intelligence and that we're law enforcement on this side of the table, so we stand where we sit and we come with a specific perspective. At the same time, we're actually deeply motivated by striking that balance. We might strike it in a bit of a different way, but we certainly appreciate the criticality of both ends of that.

If I were speculating on my own stuff—so maybe not on Mr. Dufresne's perspective—I would say that I think Canadians would be quite worried if they understood the challenges that law enforcement and intelligence have in carrying out the bread-and-butter protection of national security and the prosecution of crime in this country. To be able to do that work, we're trying to modernize in a responsible way by striking a slightly different balance, which I think has gone out of whack because legislation has been difficult to modernize, to be really frank with you.

That's how I would answer.

I'll pass it to Norm or Rick.

Normand Wong: Thank you.

I'm also not going to speculate on Mr. Dufresne's motivations for putting forward this recommendation. I will underline that part of my job at the Department of Justice is to ensure that the laws that are introduced comply with the charter. That's core to my job.

Going back to what Ms. DeBellefeuille said, the objective of this bill is to provide greater lawful access, so yes, I do have an interest in this because that's what the objective of the bill is.

There is a public outcry in this country about public safety and the crimes on the street that we're seeing. What we're hearing is that police today don't have the tools to properly do the job. I know that statistics were provided to this committee from the Canadian Centre for Child Protection in relation to how many cases get cleared, and I think they reflect how difficult it is to investigate crimes.

● (1745)

Rhonda Kirkland: I hear you, but can I just clarify something you said?

I believe you're here to provide information to us regarding this bill, but it almost sounds as though you're admitting that you're here to advocate for this bill as it's written. It sounded like that to me.

Normand Wong: I'm sorry if that's the way that it came across. Maybe I'm too invested in this bill, having lived it for the last three years.

Rhonda Kirkland: All right. Let's move on to the others. What are your thoughts?

We have to respect the Privacy Commissioner. He has a job to do, and he has done a very good job. If we don't balance it....

I don't know how many more amendments we have to look at that are recommendations from him, but if this committee continues to strike down recommendations from the Privacy Commissioner, I think we're going to be in a heap of trouble from the Canadian public.

I think we have a duty to uphold that expectation of privacy. That's why I'm asking this question very specifically of everyone. This was obviously important to the Privacy Commissioner, enough so that he gave us a recommendation for amendment. That's why I want to know from all of you why you think he would make that recommendation.

Richard Bilodeau (Acting Senior Assistant Deputy Minister, Department of Public Safety and Emergency Preparedness): Thank you for that. I'm just going to say one thing, and I think the RCMP will be able to supplement.

Putting aside the conversation about how difficult or not amending legislation can be—because that can vary, depending on the circumstances—it's not really for us to say and it's not our role to pass legislation.

We have talked about future-proofing. Part of the reason that “subscriber information” or other parts of the legislation are worded the way they are is that technology is changing fast. What might be a way of identifying a subscriber today—name, address, email and phone number—is relevant today and works today, but if it were an exclusive list, that might limit police in identifying a suspect in a specific crime during the course of an investigation, even when there were other ways of identifying the person.

That can be a limiting factor in real time because technology changes so quickly. There are probably even things that exist today in technology that speak to identifying subscriber information that aren't listed here. There's a real on-the-ground impact, and the RCMP can speak to that, but things evolve so quickly that even if you were doing legislation super quickly, it could have real impacts on real investigations.

Richard Burchill: I would add that I, too, am not going to speculate as to why the Privacy Commissioner has put forward what he's put forward.

From a law enforcement perspective, I can say that we're looking for, as the bill started off saying, timely access to information at the beginning of an investigation involving a crime and a victim. I can say with assurance that there are no investigators who are looking to have evidence that is not charter-compliant as part of their file and then going to court, giving disclosure and having the case thrown out.

From a law enforcement perspective, we're looking at the guardrails and the balances in the legislation as proposed so that we can advance investigations, because although the Privacy Commissioner has a mandate that he's speaking to, law enforcement's mandate is public protection and doing successful criminal investigations for victims of crime. The fact of the matter is that technology is an integral part of all investigations in this day and age.

Rhonda Kirkland: Thank you. I do appreciate that.

I'm what you would call a typical law-and-order Conservative, so I am completely with you in terms of how we can make it so that you can catch the bad guys, but we still have to balance the privacy of Canadians. We would be doing ourselves a disservice if we didn't do that.

I guess what I was hoping I would hear from the witnesses here in terms of why you thought Mr. Dufresne would recommend these amendments was that his motivations are to defend the privacy rights of Canadians, because that is the answer. That's why he made the recommendations. It's to defend the privacy rights of Canadians.

With the permission of the committee, I really believe we need the Privacy Commissioner in our future meetings. I don't see any reason the committee would have anything against this. I don't know how to present it. Perhaps it's a unanimous consent motion to ask that the Privacy Commissioner be invited to appear for the remainder of our clause-by-clause meetings.

● (1750)

The Chair: Unfortunately, we can't submit any motions at this time. We already have one.

Rhonda Kirkland: Can we get consent of the committee to invite the Privacy Commissioner for the remainder of clause-by-clause?

The Chair: I doubt there would be unanimous consent, and it's not possible from a procedural perspective.

Frank Caputo: I have a point of order, Mr. Chair

Just to elaborate on that, when we are no longer considering this clause, can Ms. Kirkland then move her UC motion?

The Chair: No. We're moving motion after motion, as set out in the agenda.

Frank Caputo: Okay, so her motion cannot be moved at any time throughout this meeting.

The Chair: No, not as we proceed through clause-by-clause.

Go ahead, please.

Rhonda Kirkland: I'm sorry, but may I....? There was something you said just a moment ago. I just have a question. You said that you doubt we would have unanimous consent.

The Chair: Well, that comment is irrelevant because we don't have the opportunity to discuss other motions—

Rhonda Kirkland: We're not allowed to.

Are you, Chair, allowed to invite the Privacy Commissioner to attend the remainder of the meetings?

The Chair: No. I don't decide things on my own, and we currently have a motion, which is the amendment under consideration.

Do you want to continue, MP Kirkland? Otherwise, we have MP Au and MP Mantle.

Jacob Mantle: I have a point of order, Mr. Chair.

I'm sorry, but I'm confused by your advice here. My understanding is that the committee is master of its own process in all things. Does the committee have a routine motion that would prevent it from doing UC right now? If not, then the committee is free to consider that. I'm confused.

The Chair: No, it's part of the procedures of the House and that we adopted earlier, in June last year.

If you want to conclude, go ahead, Ms. Kirkland, or I'll turn to MP Au.

Jacob Mantle: I'm sorry, but I'm not finished on that point of order, Mr. Chair. You said there was a routine motion adopted by this committee earlier on this. What motion would prevent the committee from considering UC right now?

The Chair: The committee business decisions that we made last June state explicitly that we move motion after motion. We have a motion now, so you may want to continue—

Rhonda Kirkland: I'm sorry, but can you say that again?

The Chair: We have a motion now. The next motion will be another amendment, and then there will be a clause, a motion and so on, until we finish—

Rhonda Kirkland: Yes, so we put motion after motion. Could I insert a motion between two motions?

The Chair: We have a set of motions ongoing. We discussed that earlier in the consideration of the previous bill.

Jacob Mantle: It's a subamendment to have the Privacy Commissioner.

Rhonda Kirkland: I have some real questions about that, and I may bring a point of order up later regarding this.

Thank you.

The Chair: MP Au, go ahead.

Chak Au (Richmond Centre—Marpole, CPC): Thank you.

Originally, I had questions that I wanted to ask later, but since some of my concerns have already been raised and discussed here, I have decided to ask some of these questions.

One thing that I've been struggling with so far is how we delineate grounds to believe and grounds to suspect. How do we distinguish where it would begin and where it would stop? That has been my struggle all this time.

Sergeant Gilkes, I'm grateful that you used concrete examples. That is what I need because I'm a concrete sequential learner. I need stories, facts and examples to help me understand.

Early on you gave a very good example about somebody discovering that his bicycle had been stolen. You said all the descriptions were pointing to one person, and there were reasonable grounds to suspect and have the guy investigated.

Let me give you one real case in Richmond, which happened many years ago, to see how the core suspect would fit into your description or classification.

There is a resident in my riding, in my neighbourhood, actually. He was a gardener. He spent lots of time gardening. He had a beautiful garden. One day, he discovered that his garden had been destroyed, so he made a report to the police. He said, “It is likely to be my neighbour, for the reason that he said he didn't like my garden. He hates me for gardening. I know this because each time I'm gardening, he comes to the fence and yells at me.”

He said that he didn't understand what the neighbour was talking about, but when he stopped, rose and went back to his house, the neighbour would be quiet. Not only that, he said that he received phone calls in the middle of the night. When he would pick up, somebody would yell in a very loud voice, in a different language that he didn't understand. Then he would hang up.

In that kind of situation, how would you classify the neighbour living next door? Is there reasonable grounds to suspect or reasonable grounds to believe?

● (1755)

Aaron Gilkes: Thank you for your question, Mr. Chair.

It's a very specific question. That would depend on my frame of mind at that time. The thing is, it becomes almost moot because it's going to be up to the judge or justice to decide at that point whether that's a grounds to suspect—I mean, if we were going for subscriber information.

In terms of whether that would be grounds for confirmation, do we believe that there is an offence that has been committed? Based on what you've described, there is a possibility that a crime has been committed. If that is the case, then information that I obtain based on questioning....

To be honest, I'm not sure who I would put that question to if it were for a confirmation of service. In that case, if I believed the information that was provided to me could further my investigation, that would be a good example of something that would be at a threshold of potential.

Chak Au: I'm asking a simple question. In a case like that, from the perspective of the police or investigator, are there grounds to believe or grounds to suspect?

Aaron Gilkes: It's entirely up to the investigators themselves. They have to take whatever circumstances they have and come to their own determination on whether this is something that they believe has been an offence or not. That could be from visiting the property and from seeing the type of damage that has been done.

The intention is always to corroborate. Police cannot necessarily advance an investigation without trying to corroborate whatever information has already been received, or whatever information they are receiving. It would be up to that investigator to take the steps necessary to try to corroborate whatever statement they're receiving from a victim or a potential victim.

Chak Au: Well, it's more confusing now. You seem to imply that this is subjective, depending on the interpretation of the investigator.

Aaron Gilkes: This is accurate. It is subjective, and it depends on, I guess, the vehicle that is being adopted. It's subjective for the police officer to decide.

If it's a confirmation of service, it's up to them to decide whether they have reasonable grounds to suspect. If they're going for a subscriber information production order, in that case, it'll be up to a member of the judiciary to decide whether they've reached the threshold that would be necessary. It's the same thing for reasonable grounds to believe. It depends on....

It really is subjective, because these are the people who are making a decision on whether something has reached that threshold or not.

● (1800)

Chak Au: Again, I find this very interesting.

When we are going to create a law or legislation, is it not our goal or our objective to try to eliminate the subjectivity of interpretation?

Aaron Gilkes: I won't speak to the objective of the laws themselves, but these are concepts that are already well ingrained in the Criminal Code that police work off and have worked off for many years.

Chak Au: You just said that it is quite subjective.

Now let me tell you what exactly happened and why I'm so worried that if we are not clear about the distinctions or the definitions, we can create problems. What actually happened was that this person's neighbour is a chiropractor, so when he saw his neighbour kneeling down to work on the ground, he was concerned. That's why he came to the fence and yelled at the person and said, “Come on, get up. You know it hurts your back”, and things like that.

When that person went back to the house, he was so happy, and later it was discovered that the phone call that this person received at night was an overseas call, an international call from another country, and because of a difference in the time zones, he received a call at night from a person who was mistaken and made a phone call to a wrong number from a time zone where it was daytime. All of these things could be reasonable. All these things could be misunderstood. That's why I'm so concerned about the—for lack of a better word—failure to make a clear definition.

Now let me ask you about another concrete example. Again you receive a call or a complaint saying that something has happened, and the person gives you a description of five features of the suspect—five things. Then the police are able to locate a person that fits all five features. Are there grounds to believe or grounds to suspect that this person is involved?

Richard Burchill: On that question, what I would say, not to oversimplify the process, is that the investigator—and I think this is what Sergeant Gilkes was getting at—has to do a lot of work in getting to his determination where he feels he's met reasonable grounds to suspect and is at the point where he can draft an affidavit and go before a judge.

On the face of it, it's a subjective decision to say that this is your suspect. What he'll be saying is, “I've interviewed people in the neighbourhood and I've done all my follow-up. I've done a whole bunch of investigational work to get to a point where I feel there's potential that this crime occurred, and I need more information. That's the suspect.” However, the investigator doesn't decide if that's the case. The judge decides whether the constellation of facts that have been presented in the affidavit meets what he or she feels are reasonable grounds to suspect and to grant the production order for a specific kind of information.

Just to clarify the subjectivity of it, any investigator in any police force, not just in Canada, has to get to a point where they've done enough work to determine that they suspect or believe that they have something to go to court with.

Chak Au: In this case, what the government is trying to seek is the power to not involve the judge. You want the power to get information on that person faster and more easily and without any kind of check. Is that not the case? The judge is not involved in the example that I gave.

Richard Burchill: No, that's not the case.

For a production order for subscriber information, there needs to be an affidavit. You have to go before a justice or a judge for them to determine whether you've provided enough facts to get that production order. At the beginning of an investigation, you're trying to determine.... You've figured out that there's a crime, and now you're trying to link that crime to someone. It's not subjective and it's not without process.

● (1805)

Chak Au: Are you not trying to get lawful access to information on the people that you have reason to suspect?

Richard Burchill: Exactly—

Chak Au: Exactly, so the judge is not involved.

Richard Burchill: No. The production order is for a smaller group of identifiers. It's the beginning of the investigation. You're trying to get a simpler set of information, as opposed to a general production order. For that, you need a much higher threshold and you get access to a bunch of information, some of which you probably don't need.

Again, going back to timely access for law enforcement at the beginning of an investigation, that's what the tools are, but it's not without process.

Chak Au: My question is actually this: How wide is the net you're going to open in the beginning?

Richard Burchill: I'll ask my colleagues from the Department of Justice to articulate, but I think the purpose of these tools is to narrow that scope at the beginning as you start your investigation.

Chak Au: This is what I'm trying to get at. I want to see how wide or narrow the net is going to be in the beginning of the process. I understand that when there's further investigation, there are more hurdles, so to speak, in the process, but what I am worried about is the beginning.

To continue with my example, five of the person's features fit. Is that reasonable grounds to believe or suspect?

Richard Burchill: I would say that's impossible to say without being involved in the investigation, because I haven't questioned anyone and I am not part of.... I don't know what the facts surrounding those five attributes are. I would have to do some investigation to decide.

Chak Au: Make it up: age, gender, colour, outfit and height.

Richard Burchill: I couldn't speculate on limited information.

Chak Au: Okay, let me go on. I'm using this example to try to understand.

I would assume that if this person fits all five descriptions, it's reasonable to say that he is a suspect. There are reasonable grounds to believe that he was the guy. There are reasonable grounds to believe, but if it's down to four, down to three, down to two, down to one, then I would say that perhaps when it is down to one, he would be classified as reasonable to suspect. Five are enough to believe; one is enough to suspect.

Would that be reasonable?

Richard Burchill: Again, you'd have to prepare an affidavit with facts for a judge around that one attribute. It is very difficult to say in the hypothetical.

Chak Au: This is not hypothetical. It could happen in real life.

What I'm trying to ask is, how do you draw the line? It can open up a big net that can catch almost anybody with a limited feature that fits the description.

How can we avoid that kind of situation from coming up? How can we avoid the situation of investigating somebody just based on the most basic, limited information?

Richard Burchill: We go back to the fact that the police still have to do work behind the information, even if it's basic, to be able to prove to a justice that they have enough to get more information. From the example you're giving....

I appreciate what you're trying to say. You're saying a subjective decision and a whole net of information could be gathered based on one factor. What I'm saying is that I don't think that would be reality from a policing perspective, because I have to go before a justice with an affidavit that lays out the facts that say why I believe I should be entitled to this charter-compliant information.

There are guardrails, checks and balances in the way that we get that narrow bit of information at the very beginning, at the very outset of a criminal investigation. In your example, I couldn't say what an investigator could build around one attribute.

● (1810)

Chak Au: I just want to say that I share Madame DeBellefeuille's concern around whether or not you're going on a fishing expedition.

I want to ask you another question.

Again, my colleague MP Mantle asked a question about why we would use the word “including”, which opens up the net again. Instead of using the word “including", why not use the words “limited to”? You want some concrete information—the name, the address, or a few things. Why don't you list those concrete things that you think you need and use the words “limited to”, instead of including these things and opening up the net?

Normand Wong: Thank you for the question.

As I mentioned before, the definition of subscriber information is modelled on international definitions for the same information. The way that it's been constructed, if you were to limit those things that are supposed to be examples of the types of information that are listed in proposed paragraphs (a), (b) and (c), you'd have to rewrite the definition to make sure that you don't forget obvious elements that fit under there.

For example, for identifying information, you'd want the name and address, but you may want other identifiers. In terms of what's currently before the committee right now, I think that if that suggestion were to take root, the definition would have to be recast and redrafted to make sure that all of the obvious identifiers in those classes are listed, so it would look completely different from what it does now.

Chak Au: Okay. All along, I was under the impression that the information that you are seeking is just primary information, limited and categorized as insignificant—it's not a big deal to have that kind of information.

If it is so insignificant, why would you need a law to compel the companies to give you this information? It's not voluntary; you compel them to do it.

Normand Wong: Thanks again for the question. I think that's a good policy question in terms of the mechanism.

Prior to 2014, most of this information was available to police without a warrant because it was seen as being so low threshold. Since the Supreme Court of Canada decision in R v. Spencer, there's been a lot more privacy interest attached to subscriber information, and police have had to use a judicial order to get it because there was nothing else.

Mr. Mantle mentioned Bill C-30. That was a government attempt at codifying a scheme to obtain subscriber information under an administrative scheme. There have been many attempts by various governments to do this, but you make a good point. The decision by the government was to choose a judicial order for this because they thought it would probably be the path of least resistance. Previous governments have tried an administrative scheme for this, and it didn't work.

Chak Au: Mr. Chair, I have no further questions for now.

The Chair: Thank you, MP Au.

We have MP Mantle and MP Kirkland.

Rhonda Kirkland: I have a point or order.

I was getting sleepy, but those were good questions from my colleague. I think we had three final questions.

For the benefit of the chair, I wasn't moving a motion earlier. I just wanted to make that clarification. I was simply requesting unanimous consent, which is not debatable and votable—I understand that. I also understand that it's not really up to the chair to deny consent. It's up to the committee members to deny consent.

I would like to request consent from this committee to invite the Privacy Commissioner. I have a reason for that. When I asked the question, folks on this panel were not able to tell me why they thought.... We're wondering why the Privacy Commissioner made recommendations, but he's not here to tell us why. None of us can articulate why. We have members who are here trying to explain to us how this bill is going to be good for us. For the balance, I'm requesting that the committee give unanimous consent to have the Privacy Commissioner join us for the rest of clause-by-clause after this meeting.

● (1815)

The Chair: Good. Let's see whether there is unanimous consent to move and adopt this motion.

Jacques Ramsay: Can we suspend for two minutes?

The Chair: Yes, we will suspend for two minutes.

I have a clock in front of me, so let's do that for two minutes.

● (1815)

_____(Pause)_____

● (1815)

[*Translation*]

The Chair: We'll resume the meeting.

The question is the following. Is there unanimous consent of the committee for this motion to be moved?

Jacques Ramsay: No.

The Chair: So, we'll continue.

[*English*]

Monsieur Mantle, it's your turn.

Jacob Mantle: Thanks very much, Mr. Chair.

I thought that was a pretty reasonable request. Unfortunately, to see all the Liberal members say no at the same time is pretty disappointing. We're specifically—

Yes, make faces. Make faces, Ms. Dandurand, about an important bill about lawful access. That's great. I'm glad you're taking this very seriously.

An hon. member: [*Inaudible—Editor*]

The Chair: Mr. Mantle—

Jacob Mantle: She just did.

The Chair: Mr. Mantle, I have to interrupt you, please.

An hon. member: [*Inaudible—Editor*]

The Chair: Okay. Thank you—

Jacob Mantle: I'm not tired and irritated at all.

Some hon. members: Oh, oh!

The Chair: Mr. Mantle and everyone in the room, please—

Jacob Mantle: She can speak for herself.

An hon. member: [*Inaudible—Editor*]

The Chair: I'm going to suspend.

● (1815)

_____(Pause)_____

● (1820)

[*Translation*]

The Chair: We'll resume the meeting.

Mr. Mantle, you have the floor.

[*English*]

Jacob Mantle: That was quick.

Thank you, Mr. Chair.

I would move that we suspend consideration of this clause until the Privacy Commissioner can be invited to attend.

The Chair: This is a dilatory motion, which we're going to vote on immediately. The motion is to adjourn this debate. Is anyone in favour of that?

Jacob Mantle: I said to stay the clause, not to adjourn. It's not a dilatory motion.

The Chair: You want to stay the clause...?

Jacob Mantle: Yes, I want to stay the clause until we can invite the Privacy Commissioner to attend.

The Chair: Okay, I'm sorry. I misunderstood what you said.

There is a motion to stay the clause, which means that, in practice, we would put consideration of this clause—or amendment BQ-3—later in the process.

It can't be....

Anthony Housefather: I have a point of order.

The Chair: We'll have to suspend because we can't do that for any particular amendment. We'll have to check with the legislative clerk to see if this is possible.

● (1820)

_____(Pause)_____

● (1820)

[*Translation*]

The Chair: We'll resume the meeting.

The motion is to delay the discussion on clause 4 and to come back to it later during the clause-by-clause consideration of the bill.

Does the committee give its unanimous consent?

Some hon. members: No.

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

[*English*]

Jacob Mantle: Thank you.

I guess this is a point of order, though. Your description of my request was not accurate. It was conditional. It wasn't simply to delay consideration of the clause. It was to delay consideration of the clause until the Privacy Commissioner could be present for that.

The Chair: The motion was defeated. We can vote on the motion again, if you want.

Jacob Mantle: Okay. I'd like a recorded vote.

[*Translation*]

The Chair: Okay.

Mr. Mantle, you're moving a motion to delay the consideration of the clause and to come back to it later during the clause-by-clause consideration of the bill, after the Privacy Commissioner has been invited.

We'll now proceed to a recorded division on this matter.

(Motion negatived: nays 6; yeas 5)

The Chair: Mr. Mantle, do you have anything else to add?

[*English*]

Jacob Mantle: Yes, I believe I'm on the speaking list next. Thank you, Mr. Chair.

Returning to BQ-2, I'd like to move a subamendment.

● (1825)

The Chair: We're on BQ-3.

Jacob Mantle: It's on BQ-3. I apologize.

I'd like to move a subamendment to BQ-3 that would delete the word “including” in proposed paragraph (a) and also delete the word “including” in proposed paragraph (b). Is that clear?

The Chair: No, we need that in writing.

Jacob Mantle: Then I'll need a moment to put that in writing to provide to the clerk. Can we suspend? It's just removing two words.

The Chair: Yes, but it's just to make sure that everything is well understood by everyone.

We'll suspend for whatever little time is needed for that to be shared.

● (1825)

_____(Pause)_____

● (1825)

[*Translation*]

The Chair: I would like to inform you right now that I'll be adjourning the meeting since it's 6:30 p.m. We need to do a proper job on the subamendment.

Thank you and good evening.